Union internationale des télécommunications

Sécurité dans les télécommunications et les technologies de l'information

Aperçu des problèmes et présentation des Recommandations UIT-T existantes sur la sécurité dans les télécommunications

UIT-T

UIT-T

Secteur de la normalisation des télécommunications de l'UIT

2006



UIT-T – Bureau de la normalisation des télécommunications (TSB)
Place des Nations – CH-1211 Genève 20 – Suisse
E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T

Sécurité dans les télécommunications et les technologies de l'information

Aperçu des problèmes et présentation des Recommandations UIT-T existantes sur la sécurité dans les télécommunications

Juin 2006

Remerciements

De nombreuses personnes ont participé à la préparation de ce manuel, en contribuant à l'élaboration de Recommandations UIT-T pertinentes ou en participant à des réunions des Commissions d'études de l'UIT-T, à des ateliers ou à des séminaires. Il convient en particulier de rendre honneur aux personnes suivantes: Herb Bertine, David Chadwick, Martin Euchner, Mike Harrop, Sándor Mazgon, Stephen Mettler, Chris Radelet, Lakshmi Raman, Eric Rosenfeld, Neal Seitz, Rao Vasireddy, Tim Walker, Heung-Youl Youm, Joe Zebarth, ainsi qu'aux conseillers du TSB/UIT.

Table des matières

Page

Préface

Jusqu'à encore récemment, la sécurité dans les télécommunications et les technologies de l'information concernait principalement des domaines spécialisés tels que les applications bancaires, aérospatiales et militaires. Toutefois, avec la croissance rapide et généralisée de l'utilisation des communications de données, et notamment de l'Internet, la sécurité est devenue l'affaire de presque tous.

L'ampleur prise par la sécurité des technologies de l'information et des communications (TIC) peut être attribuée en partie à des incidents qui ont défrayé la chronique tels que des virus, des vers, des piratages et des menaces d'atteinte à la vie privée. Toutefois, les ordinateurs et les réseaux font désormais tellement partie de la vie quotidienne, qu'il est impératif de mettre en place des mesures de sécurité efficaces afin de protéger les systèmes informatiques et de télécommunications des pouvoirs publics, des entreprises, des sociétés de commerce, des infrastructures critiques et des particuliers. Par ailleurs, de plus en plus de pays disposent maintenant d'une législation de protection des données qui exige le respect des normes éprouvées de confidentialité et d'intégrité des données.

Il est primordial que le processus de sécurité soit bien conçu à toutes les étapes, depuis la définition et la conception des systèmes jusqu'à leur implémentation et leur déploiement. Lors de l'élaboration de normes, la sécurité doit toujours être prise en considération dès le départ, et non ultérieurement. Faute de prendre en compte correctement la sécurité au cours de la phase de conception lors de l'élaboration de normes et de systèmes, il en résulte facilement des vulnérabilités au niveau de son implémentation. Les comités de normalisation ont un rôle essentiel à jouer dans la protection des systèmes informatiques et de télécommunications en se tenant au courant des problèmes de sécurité, en faisant en sorte que les considérations de sécurité constituent une partie fondamentale des spécifications et en donnant des indications aux personnes chargées de l'implémentation et aux utilisateurs afin de les aider à rendre les systèmes et services de communication suffisamment fiables.

L'UIT-T participe activement aux travaux dans le domaine de la sécurité pour les télécommunications et les technologies de l'information depuis de nombreuses années. Toutefois, il n'est pas toujours facile de déterminer quels sujets ont été traités et dans quels documents ils l'ont été. Le présent manuel vise à rassembler toutes les informations disponibles sur les travaux réalisés par l'UIT-T.

Le manuel est destiné à guider les techniciens, les cadres intermédiaires ainsi que les organes de réglementation dans l'implémentation pratique des fonctions de sécurité. A travers plusieurs exemples d'applications, les problèmes de sécurité sont expliqués, l'accent étant mis sur la manière dont ils sont pris en considération dans les Recommandations de l'UIT-T.

La première version de ce manuel, datée de 2003, a été publiée en décembre 2003, avant la première phase du Sommet mondial sur la société de l'information (SMSI). L'accueil enthousiaste qui lui a été réservé par la communauté des TIC dans le monde entier ainsi que les propositions et réactions utiles qui ont été communiquées par les lecteurs nous ont encouragés à élaborer une deuxième version. La version publiée en octobre 2004 comportait une nouvelle structure avec des informations additionnelles et certains domaines ont été étoffés. Cette troisième version, datée de 2006, tient compte de la nouvelle structure des Commissions d'études et des Questions qui a été adoptée à l'Assemblée mondiale de normalisation des télécommunications tenue à Florianópolis du 5 au 14 octobre 2004 (AMNT-04).

J'exprime toute ma gratitude aux ingénieurs du Bureau de la normalisation des télécommunications de l'UIT qui, conjointement avec des experts provenant d'Etats Membres de l'UIT, ont élaboré la plus grande partie de la première version. J'exprime également toute ma gratitude à ceux qui nous ont communiqué des propositions utiles et à ceux qui ont contribué à la nouvelle version. Mes remerciements vont en particulier à M. Herbert Bertine, Président de la Commission d'études 17 de l'UIT-T (Commission d'études directrice pour la sécurité) ainsi qu'à l'équipe de collaborateurs de la Commission d'études 17 et des autres Commissions d'études de l'UIT-T.

Je suis certain que ce manuel sera utile à tous ceux qui s'intéressent aux problèmes de sécurité et j'invite les lecteurs à me communiquer leurs réactions en vue des éditions futures.

Houlin Zhao

Directeur du Bureau de la normalisation des télécommunications de l'UIT

Genève, juin 2006

Résumé

Le secteur des télécommunications a largement contribué à l'amélioration de la productivité et de l'efficacité mondiales avec l'élaboration d'infrastructures de communications qui mettent en relation les communautés dans presque tous les secteurs industriels et dans chaque partie du monde. Cela a été possible, en grande partie, grâce à l'implémentation de normes élaborées par des organismes tels que l'UIT-T. Ces normes permettent non seulement de garantir l'interopérabilité des réseaux et l'efficacité de leur exploitation mais aussi de jeter les bases des réseaux de prochaine génération (NGN, *next generation network*). Toutefois, tandis que les normes continuent de répondre aux besoins des utilisateurs finals et de l'industrie, l'utilisation croissante d'interfaces et de protocoles ouverts, la multiplicité des nouveaux participants, la diversité même des applications et des plates-formes et le fait que les implémentations ne sont pas toujours testées correctement ont augmenté les risques d'utilisation malveillante des réseaux. Ces dernières années, on a observé une forte augmentation des violations de la sécurité (virus et attaques ayant entraîné des atteintes à la confidentialité de données enregistrées par exemple) dans les réseaux mondiaux, entraînant souvent de graves conséquences économiques. La question est alors de savoir comment prendre en charge une infrastructure de télécommunication ouverte sans compromettre les informations échangées sur cette infrastructure. Une grande partie de la réponse tient à l'élaboration de spécifications suffisamment robustes pour faire en sorte que les menaces de sécurité puissent être contrées, quelle que soit la partie de l'infrastructure de communication visée par ces menaces. Cet objectif étant fixé, les efforts des groupes de normalisation doivent porter sur la définition d'architectures et de cadres de sécurité normalisés, sur l'élaboration de normes de gestion de la sécurité, sur la mise au point de protocoles et de techniques propres à la sécurité afin de sécuriser les protocoles de communications ainsi que sur la définition d'étapes à suivre pour minimaliser les vulnérabilités potentielles dans les normes de communications d'une manière générale.

Ce manuel sur la sécurité vise à donner un aperçu des nombreuses Recommandations élaborées par l'UIT-T – parfois en collaboration avec d'autres organismes de normalisation – en vue de sécuriser l'infrastructure des télécommunications ainsi que les services et applications associés.

Pour aborder les multiples aspects de la sécurité, il faut établir un cadre et une architecture afin de définir un vocabulaire commun qui servira de base à l'examen des concepts.

Le paragraphe 2 présente les architectures et éléments de sécurité de base définis dans les Recommandations de l'UIT-T ainsi que les huit dimensions de sécurité qui ont été définies afin d'assurer la sécurité de bout en bout des applications de réseau – respect de la vie privée, confidentialité des données, authentification, intégrité des données, non-répudiation, contrôle d'accès, sécurité des communications et disponibilité. Ces principes généraux servent de base à bon nombre des autres normes relatives aux services et aux mécanismes de sécurité.

Le paragraphe 3 présente les concepts de sécurité fondamentaux que sont les menaces, les vulnérabilités et les risques, et explique les relations entre ces concepts et précise le rôle des organismes de normalisation en rapport avec ces concepts.

Le paragraphe 4 s'appuie sur les informations données dans les paragraphes précédents pour définir les exigences de sécurité pour les réseaux de télécommunication. Il traite en particulier des objectifs de sécurité pour les réseaux de télécommunication et des services qui peuvent être utilisés pour atteindre ces objectifs.

Le paragraphe 5 présente les concepts importants d'infrastructure de clé publique et d'infrastructure de gestion de privilège. Ces infrastructures ainsi que leurs mécanismes sous-jacents sont particulièrement importants dans la prise en charge des services d'authentification et d'autorisation.

L'UIT-T a élaboré des dispositions relatives à la sécurité de plusieurs systèmes et services définis dans ses Recommandations et une grande partie de ce manuel – le paragraphe 6 – porte sur des applications. Parmi les applications présentées figurent la téléphonie et les applications multimédias sur IP (H.323 et IPCablecom), la télésanté et la télécopie. Pour ces applications, on décrit l'architecture de déploiement et la manière dont les protocoles ont été définis pour répondre aux besoins de sécurité. Il faut non seulement assurer la sécurité des informations relatives aux applications, mais aussi sécuriser l'infrastructure du réseau et la gestion des services de réseau. Le paragraphe 6 contient donc aussi des exemples de normes dans lesquelles figurent des dispositions en matière de sécurité de la gestion de réseau.

Le paragraphe 7 porte sur la dimension de sécurité disponibilité et sur la couche de sécurité infrastructure, deux des domaines de compétence essentiels de l'UIT-T même s'ils ne sont pas toujours considérés comme contribuant à la sécurité. Ce paragraphe contient des informations sur le calcul de la disponibilité et sur les moyens permettant d'améliorer la disponibilité d'un réseau de transport. En conclusion, il donne des indications concernant la sécurisation des installations extérieures.

Le paragraphe 8 présente les lignes directrices que l'UIT-T a approuvées récemment concernant l'organisation en cas d'incident et la prise en charge des incidents relatifs à la sécurité. Il est généralement admis que cette question est extrêmement importante compte tenu de la multiplication des menaces de sécurité visant l'infrastructure des systèmes de télécommunication et d'information.

De plus, ce manuel contient la version actuelle du catalogue des Recommandations de l'UIT-T relatives à des aspects de sécurité – la liste donnée dans l'Annexe A est longue, ce qui est à l'image de l'étendue des travaux de l'UIT-T sur la sécurité. Ce manuel contient aussi une liste d'acronymes et de définitions liés à la sécurité et à d'autres thèmes abordés dans ce document, extraits de Recommandations de l'UIT-T et d'autres sources (telles que la base de données SANCHO de l'UIT-T et le recueil de définitions relatives à la sécurité approuvées par l'UIT-T, élaboré par la Commission d'études 17 de l'UIT-T). Cette liste figure dans l'Annexe B. L'Annexe C résume les tâches liées à la sécurité auxquelles chacune des Commissions d'études de l'UIT-T est attelée. Les informations contenues dans ces annexes sont constamment mises à jour et figurent à l'adresse www.itu.int/ITU-T.

En conclusion, l'UIT-T agit par anticipation, non seulement en ce qui concerne les technologies fondées sur IP mais aussi pour ce qui est de répondre aux besoins de nombreux secteurs industriels différents, dans lesquels les exigences de sécurité sont très variables. Ce manuel montre que les Recommandations de l'UIT-T offrent des solutions non seulement en termes de cadre et d'architecture génériques mais aussi pour des systèmes et des applications spécifiques qui sont déjà déployés à l'échelle mondiale par des fournisseurs de réseaux et de services.

1 Domaine d'application du manuel

Ce manuel donne un aperçu de la sécurité dans les télécommunications et les technologies de l'information, décrit des problèmes pratiques et indique comment l'UIT-T aborde les différents aspects de la sécurité dans les applications actuelles. Il a une portée didactique: il rassemble en un même endroit les informations relatives à la sécurité contenues dans les Recommandations de l'UIT-T et explique les relations respectives. Le manuel porte sur d'autres aspects de la sécurité, notamment sur les aspects liés à la disponibilité, pour lesquels l'UIT-T a beaucoup à offrir, ainsi que sur les dommages causés par l'environnement, domaine dans lequel l'UIT-T travaille également. Il fait aussi le point sur les efforts de normalisation dans le domaine de la sécurité qui ont été menés à leur terme depuis la deuxième édition. Par ailleurs, les aspects traités sont fondés sur les travaux déjà réalisés, et non pas sur les travaux en cours, qui feront l'objet de futures éditions de ce manuel.

Ce manuel est destiné aux ingénieurs et aux chefs de produit, aux étudiants et au monde universitaire ainsi qu'aux organes de réglementation qui souhaitent mieux comprendre les problèmes de sécurité dans les applications pratiques.

2 Architectures et services de sécurité de base

Au cours des travaux de normalisation des télécommunications réalisés au début des années 1980, il a été reconnu qu'il fallait s'intéresser à des éléments d'architecture de sécurité. C'est alors qu'a été définie l'architecture de sécurité pour les systèmes ouverts (Rec. UIT-T X.800). Toutefois, il a également été reconnu qu'il ne s'agissait que de la première étape de l'élaboration d'une série de normes relatives aux services et mécanismes de sécurité. Ces travaux, menés en grande partie en collaboration avec l'ISO, ont conduit à l'élaboration d'autres Recommandations, notamment sur les modèles et cadres de sécurité qui spécifient comment des types de protection particuliers peuvent être appliqués dans des environnements particuliers. En outre, il s'est avéré nécessaire de définir d'autres architectures de sécurité, par exemple les architectures de sécurité pour le traitement réparti ouvert et pour les systèmes assurant des communications de bout en bout. La Rec. UIT-T X.805, publiée récemment, répond à cette nécessité et complète les autres Recommandations de la série X.800 en offrant des solutions destinées à assurer la sécurité de réseau de bout en bout.

2.1 Architecture de sécurité pour les systèmes ouverts (X.800)

La première des architectures de sécurité pour les communications à avoir été normalisée a été l'architecture de sécurité pour les systèmes ouverts, définie dans la Rec. UIT-T X.800. Cette Recommandation définit les éléments généraux d'architecture liés à la sécurité qui peuvent être appliqués lorsqu'une protection est requise. Elle contient en particulier une description générale de services de sécurité et des mécanismes associés qui peuvent être utilisés pour assurer les services. Elle définit aussi, sur la base du modèle de référence de base à sept couches pour l'interconnexion des systèmes ouverts (OSI, *open systems interconnection*), les emplacements les plus appropriés pour implémenter les services de sécurité.

La Rec. UIT-T X.800 porte uniquement sur les aspects visibles d'une voie de communication permettant aux systèmes d'extrémité de se transférer des informations en toute sécurité. Elle ne vise pas à spécifier des implémentations particulières et elle ne définit pas la marche à suivre pour évaluer la conformité d'une implémentation donnée à cette norme sur la sécurité ou à toute autre norme sur la sécurité. Elle ne précise pas non plus les mesures de sécurité additionnelles qui pourraient être nécessaires dans les systèmes d'extrémité pour prendre en charge les fonctionnalités de sécurité OSI.

L'architecture de sécurité définie dans la Rec. UIT-T X.800 a été élaborée spécifiquement pour les systèmes OSI, mais les concepts sous-jacents se sont avérés avoir une applicabilité et une acceptation beaucoup plus larges. La norme est particulièrement importante car elle représente le premier consensus à l'échelle internationale sur les définitions des services de sécurité de base (*authentification*, *contrôle d'accès*, *confidentialité des données*, *intégrité des données* et *non-répudiation*) ainsi que de services plus généraux (omniprésents) (*fonctionnalité de confiance*,

détection d'événements, *audit de sécurité et reprise de sécurité*, etc.). Avant l'élaboration de la Rec. UIT-T X.800, les avis étaient très variés sur les services de sécurité de base nécessaires et sur les fonctionnalités exactes de chaque service. La Rec. UIT-T X.800 traduit un fort consensus international sur ces services. (Les services de sécurité de base sont examinés plus en détail au § 2.3.)

L'intérêt et l'applicabilité générale de la Rec. UIT-T X.800 tiennent spécifiquement au fait que cette Recommandation représente un consensus important sur la signification des termes employés pour décrire les fonctionnalités de sécurité, sur l'ensemble des services de sécurité nécessaires pour assurer la protection des communications de données et sur la nature de ces services de sécurité.

Au cours de l'élaboration de la Rec. UIT-T X.800, il s'est avéré nécessaire d'établir d'autres normes connexes sur la sécurité des communications. Un certain nombre de normes connexes et de Recommandations complémentaires relatives à l'architecture ont donc commencé à être mises au point après l'élaboration de la Rec. UIT-T X.800. Certaines de ces Recommandations sont examinées ci-après.

2.2 Modèles de sécurité pour les couches inférieures et pour les couches supérieures (X.802 et X.803)

Les modèles de sécurité pour les couches inférieures et pour les couches supérieures (Recommandations UIT-T X.802 et X.803 respectivement) visent à montrer comment les concepts de sécurité définis dans les cadres de sécurité peuvent être appliqués à certaines parties des architectures de systèmes ouverts.

Le modèle de sécurité pour les couches supérieures (X.803) est destiné à être le modèle architectural que les personnes chargées de normalisation doivent utiliser pour mettre au point des services et des protocoles de sécurité indépendants de l'application dans les couches supérieures du modèle OSI à sept couches. Cette Recommandation contient des indications sur le positionnement des services de sécurité et sur les relations entre ces services dans les couches Session, Présentation et Application. Elle décrit en particulier comment les fonctions de transformation pour la sécurité (chiffrement par exemple) sont traitées dans les couches Application et Présentation. De plus, elle introduit le concept d'*échange pour la sécurité*. Elle décrit également ce qu'est une *politique de sécurité* et un *état de sécurité*.

Le modèle de sécurité pour les couches inférieures (X.802) contient des indications pour la mise au point de protocoles et d'éléments de protocole liés à la sécurité qui soient appropriés pour les couches inférieures du modèle OSI. Cette Recommandation jette les bases des interactions de sécurité entre les couches inférieures et décrit le positionnement des protocoles de sécurité.

2.3 Cadres de sécurité (X.810 à X.816)

Les cadres de sécurité ont été élaborés pour pouvoir décrire de façon complète et cohérente les services de sécurité définis dans la Rec. UIT-T X.800. Ils ont pour objet de définir tous les aspects liés à l'application des services de sécurité dans le contexte d'une architecture de sécurité particulière, y compris les éventuelles architectures de sécurité qui seront définies dans le futur. Ils visent essentiellement à assurer la protection des systèmes, des objets contenus dans les systèmes et de l'interaction entre les systèmes. Ils ne traitent pas de la marche à suivre pour construire des systèmes ou des mécanismes.

Les cadres portent à la fois sur les éléments de données et sur les séquences d'opérations (à l'exclusion des éléments de protocole) qui sont utilisés pour obtenir des services de sécurité spécifiques. Ces services peuvent s'appliquer aux entités de système en communication ainsi qu'aux données échangées entre systèmes et gérées par ces systèmes.

2.3.1 Aperçu des cadres de sécurité (X.810)

L'aperçu des cadres de sécurité présente les différents cadres et décrit les concepts communs (domaines de sécurité, autorités de sécurité et politiques de sécurité) qui sont utilisés dans tous les cadres. Il décrit également un format de données générique qui peut être utilisé pour acheminer en toute sécurité les informations d'authentification et de contrôle d'accès.

2.3.2 Cadre d'authentification (X.811)

L'*authentification* est l'attestation de l'identité revendiquée par une entité. Les entités incluent non seulement les utilisateurs humains, mais aussi les dispositifs, les services et les applications. L'authentification permet aussi d'attester qu'une entité ne tente pas d'usurper l'identité d'une autre entité ni de reprendre sans autorisation une communication précédente. La Rec. UIT-T X.800 définit deux formes d'authentification: *l'authentification de l'origine des données* (à savoir la confirmation que la source des données reçues est telle que déclarée) et *l'authentification de l'entité homologue* (à savoir la confirmation qu'une entité homologue d'une association est bien l'entité déclarée).

Le cadre d'authentification occupe la position sommitale d'une hiérarchie de normes d'authentification qui définissent des concepts, une nomenclature et une classification concernant les méthodes d'authentification. Il définit les concepts de base de l'authentification, les différentes classes de mécanismes d'authentification, les services correspondant à ces classes de mécanismes, les exigences fonctionnelles que les protocoles doivent respecter pour prendre en charge ces classes de mécanismes et, enfin, les exigences générales de gestion à respecter concernant l'authentification.

L'authentification suit généralement l'identification. Les informations utilisées pour l'identification, l'authentification et l'autorisation doivent être protégées.

2.3.3 Cadre de contrôle d'accès (X.812)

Le *contrôle d'accès* est la précaution prise contre l'utilisation non autorisée d'une ressource, y compris la précaution prise contre l'utilisation d'une ressource de façon non autorisée. Le contrôle d'accès garantit que seuls les personnes ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications.

Le cadre de contrôle d'accès décrit un modèle incluant tous les aspects du contrôle d'accès dans les systèmes ouverts, la relation avec les autres fonctions de sécurité (par exemple l'authentification et l'audit) et les exigences de gestion à respecter concernant le contrôle d'accès.

2.3.4 Cadre de non-répudiation (X.813)

La *non-répudiation* est la capacité d'empêcher les entités de nier ultérieurement qu'elles ont exécuté une action. Il s'agit d'établir une preuve qui puisse ensuite être utilisée pour rejeter les fausses déclarations. La Rec. UIT-T X.800 décrit deux formes de service de non-répudiation, à savoir la *non-répudiation avec preuve de remise*, qui sert à rejeter toute fausse déclaration d'un destinataire qui nie avoir reçu des données, et la *non-répudiation avec preuve d'origine*, qui sert à rejeter toute fausse déclaration d'un expéditeur qui nie avoir envoyé des données. Toutefois, dans un sens plus général, le concept de non-répudiation peut être appliqué à de nombreux contextes différents, notamment la non-répudiation de création, de soumission, de stockage, de transmission et de réception de données.

Le cadre de non-répudiation élargit les concepts des services de sécurité de non-répudiation décrits dans la Rec. UIT-T X.800 et sert de cadre pour la définition de ces services. En outre, il définit les mécanismes possibles de prise en charge de ces services et les exigences générales de gestion concernant la non-répudiation.

2.3.5 Cadre de confidentialité (X.814)

La *confidentialité* est la propriété d'une information qui n'est ni communiquée, ni divulguée aux individus, entités ou processus non autorisés.

Le service de confidentialité a pour objet de protéger les informations contre toute divulgation non autorisée. Le cadre de confidentialité porte sur la confidentialité des informations au moment de leur extraction, de leur transfert et de leur gestion en définissant les concepts de base de la confidentialité, les différentes classes de confidentialité et les fonctionnalités requises pour chaque classe de mécanismes de confidentialité, les services de gestion et les services support requis ainsi que l'interaction avec les autres services et mécanismes de sécurité.

2.3.6 Cadre d'intégrité (X.815)

L'*intégrité des données* est la propriété de données qui n'ont pas été modifiées de façon non autorisée. En général, un service d'intégrité répond à la nécessité de garantir que les données ne sont pas corrompues ou, si elles le sont, que l'utilisateur est au courant de cette corruption. Il existe différentes formes d'intégrité (intégrité des données et intégrité des systèmes par exemple), mais la Rec. UIT-T X.800 porte presque exclusivement sur l'intégrité des données.

Le cadre d'intégrité porte sur l'intégrité des données au moment de leur extraction, de leur transfert et de leur gestion. Il définit les concepts de base de l'intégrité, les différentes classes de mécanismes d'intégrité et les fonctionnalités pour chaque classe de mécanismes, la gestion requise pour prendre en charge chaque classe de mécanismes ainsi que l'interaction du mécanisme d'intégrité et des services support avec les autres services et mécanismes de sécurité.

2.3.7 Cadre d'audit et d'alarmes (X.816)

Un *audit de sécurité* est une analyse et un examen – effectués de façon indépendante – des enregistrements et activités d'un système afin de vérifier si les contrôles du système sont adéquats, de vérifier le respect de la politique de sécurité établie et des procédures d'exploitation, de détecter les infractions à la sécurité et de recommander les modifications appropriées des contrôles, de la politique et des procédures. Une *alarme de sécurité* est un message généré lorsqu'un événement lié à la sécurité, défini par la politique de sécurité comme étant une condition d'alarme, a été détecté.

Le cadre d'audit et d'alarmes définit les concepts de base et un modèle général de l'audit et des alarmes de sécurité, les critères applicables à un audit de sécurité et à l'envoi d'alarmes, les différentes classes de mécanismes d'audit et d'alarmes, les services correspondant à ces classes de mécanismes, les exigences fonctionnelles à respecter pour prendre en charge ces mécanismes ainsi que les exigences générales de gestion concernant l'audit et les alarmes de sécurité.

2.4 Architecture de sécurité pour les systèmes assurant des communications de bout en bout (X.805)

Récemment, un nouveau regard a été posé sur l'architecture de sécurité pour les réseaux, ce qui a conduit à l'élaboration de la Rec. UIT-T X.805, qui définit une architecture de sécurité en vue d'assurer une sécurité de réseau de bout en bout. L'architecture peut être appliquée à divers types de réseaux pour lesquels on s'intéresse à la sécurité de bout en bout indépendamment de la technologie sous-jacente du réseau. Les principes généraux et les définitions s'appliquent à toutes les applications, même si les détails tels que les menaces et les vulnérabilités ainsi que les mesures visant à les contrer ou à les empêcher varient en fonction des besoins de chaque application.

Cette architecture de sécurité est définie sur la base de deux principaux concepts: les couches et les plans. Le premier axe, à savoir les couches de sécurité, se rapporte aux prescriptions qui s'appliquent aux éléments de réseau et aux systèmes qui constituent le réseau de bout en bout. On adopte une approche hiérarchique de subdivision des prescriptions entre les couches de manière à assurer la sécurité de bout en bout, couche après couche. Les trois couches sont les suivantes: la couche infrastructure, la couche services et la couche applications. La définition de couches présente notamment pour avantage de pouvoir réutiliser ces couches dans différentes applications pour assurer la sécurité de bout en bout. Les vulnérabilités au niveau de chaque couche sont différentes et il faut donc définir différentes contre-mesures pour répondre aux besoins de chaque couche. La couche infrastructure comprend les installations de transmission de réseau et les différents éléments de réseau. Elle comprend notamment les routeurs, commutateurs et serveurs ainsi que les liaisons de communication qui les relient. La couche services concerne la sécurité des services de réseau qui sont

offerts aux clients. Ces services vont des offres de connexion de base telles que les services de lignes louées aux services à valeur ajoutée tels que la messagerie instantanée. La couche applications concerne les prescriptions relatives aux applications de réseau utilisées par les clients. Ces applications peuvent être aussi simples que la messagerie électronique ou aussi complexes que la visualisation collaborative, pour laquelle des transferts vidéo très haut de gamme sont opérés dans les domaines de l'exploration pétrolière, de la conception d'automobiles, etc.

Le second axe concerne la sécurité des activités exécutées dans un réseau. Cette architecture de sécurité définit trois plans de sécurité pour représenter les trois types d'activités protégées qui ont lieu dans un réseau. Les plans de sécurité sont les suivants: 1) le plan de gestion; 2) le plan de commande; et 3) le plan d'utilisateur final. Ils visent à répondre aux besoins de sécurité particuliers associés aux activités de gestion de réseau, aux activités de signalisation et de commande de réseau et aux activités d'utilisateur final correspondantes. Le plan de gestion, examiné plus en détail au § 6.4, se rapporte aux activités d'exploitation, d'administration, de maintenance et de configuration (OAM&P, *operations, administration, maintenance and provisioning*), par exemple la configuration d'un utilisateur ou d'un réseau, etc. Le plan de commande est associé aux aspects de signalisation pour l'établissement (et la modification) de la communication de bout en bout dans le réseau, quels que soient le support et la technologie utilisés dans le réseau. Le plan d'utilisateur final concerne la sécurité d'accès au réseau et d'utilisation du réseau par les clients. Il se rapporte aussi à la protection des flux de données d'utilisateur final.

Outre les couches de sécurité et les plans de sécurité constituant les deux axes (3 plans de sécurité et 3 couches de sécurité), l'architecture définit aussi huit dimensions de sécurité concernant la sécurité de réseau. Ces dimensions sont définies ci-après. D'un point de vue architectural, ces dimensions sont appliquées à chaque cellule de la matrice 3×3 formée par les couches et les plans de manière à pouvoir déterminer les contre-mesures appropriées. La Figure 2-1 illustre les plans, couches et dimensions de sécurité de l'architecture de sécurité. Le § 6.4 portant sur le plan de gestion montre comment les trois cellules de la matrice 3×3 relatives au plan de gestion sont prises en considération dans les autres Recommandations de l'UIT-T.

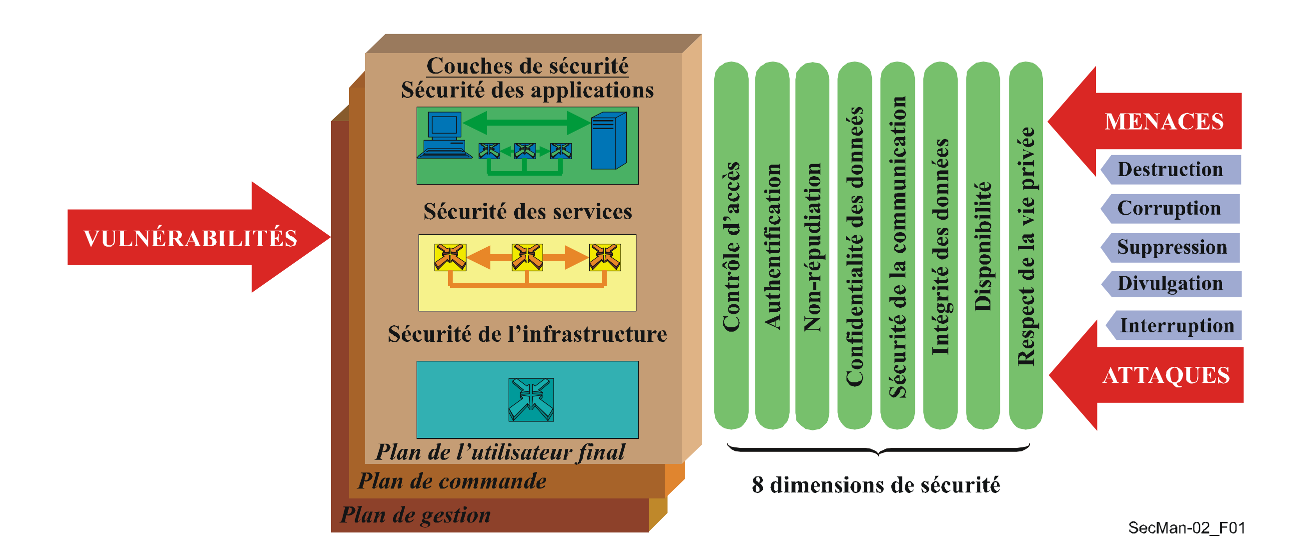


Figure 2-1 – Eléments architecturaux de sécurité (Rec. UIT-T X.805)

La Rec. UIT-T X.805 s'appuie sur certains des concepts de la Rec. UIT-T X.800 et sur les cadres de sécurité (X.810-X.816) examinés ci-dessus. En particulier, les fonctionnalités des services de sécurité de base de la Rec. UIT-T X.800 (*contrôle d'accès*, *authentification*, *confidentialité des données*, *intégrité des données* et *non-répudiation*) concordent avec les fonctionnalités des dimensions de sécurité correspondantes de la Rec. UIT-T X.805 (illustrées sur la Figure 2-1). En outre, les dimensions de sécurité *sécurité de la communication*, *disponibilité* et *respect de la vie privée* de la Rec. UIT-T X.805 offrent de nouveaux types de protection de réseau. Ces huit dimensions de sécurité sont présentées ci-après.

– La dimension de sécurité *contrôle d'accès* permet d'assurer la protection contre toute utilisation non autorisée de ressources de réseau. Le contrôle d'accès permet de garantir que seuls les personnes ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications.

– La dimension de sécurité *authentification* sert à confirmer les identités des entités qui communiquent. L'authentification permet de garantir la validité des identités déclarées des entités en communication (par exemple, une personne, un dispositif, un service ou une application) et donne l'assurance qu'une entité ne tente pas d'usurper l'identité d'une autre entité ou de reprendre sans autorisation une précédente communication.

– La dimension de sécurité *non-répudiation* permet d'empêcher une personne ou une entité de nier avoir exécuté une action particulière liée aux données, grâce à la fourniture de diverses preuves d'actions dans le réseau (par exemple une preuve d'obligation, d'intention ou d'engagement; une preuve d'origine des données, une preuve de propriété ou une preuve d'emploi de ressources). Elle permet à une preuve d'être présentée à une entité tierce et d'être utilisée pour prouver qu'un certain type d'événement ou d'action a eu lieu.

– La dimension de sécurité *confidentialité des données* permet de protéger les données contre toute divulgation non autorisée. La confidentialité des données permet de garantir que le contenu des données ne pourra être compris par des entités non autorisées. Le chiffrement, les listes de contrôle d'accès, et les permissions d'accès aux fichiers sont des méthodes souvent employées pour assurer la confidentialité des données.

– La dimension de sécurité *sécurité de la communication* permet de garantir que les informations ne seront acheminées qu'entre les points d'extrémité autorisés (les informations ne sont ni déviées ni interceptées au cours de leur acheminement entre ces points).

– La dimension de sécurité *intégrité des données* permet de garantir que les données sont correctes ou exactes. Les données sont protégées contre toute modification, suppression, création et reproduction non autorisées. Ces activités non autorisées sont signalées.

– La dimension de sécurité *disponibilité* permet de garantir qu'il n'y a pas déni de l'accès autorisé aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau. Les solutions de récupération en cas de catastrophe sont comprises dans cette catégorie.

– La dimension de sécurité *respect de la vie privée* permet d'assurer la protection des informations qui pourraient être obtenues à partir de l'observation des activités dans le réseau. Ces informations sont par exemple les sites web que l'utilisateur a visités, l'emplacement géographique de l'utilisateur, ainsi que les adresses IP et les noms DNS des dispositifs présents dans le réseau d'un fournisseur de services.

L'architecture de sécurité X.805 peut servir de guide pour élaborer des définitions de politiques de sécurité détaillées, des plans de réaction aux incidents et de récupération, ainsi que des architectures technologiques, en tenant compte, au cours de la phase de définition et de planification, de chaque

dimension de sécurité au niveau de chaque couche et de chaque plan de sécurité. L'architecture de sécurité X.805 peut aussi servir de base à une évaluation de la sécurité qui serait faite pour examiner comment l'implémentation du programme de sécurité tient compte des dimensions, des couches et des plans de sécurité, lorsque les politiques et les procédures sont mises en œuvre et que la technologie est déployée. Dès qu'un programme de sécurité a été mis en place, il doit être tenu à jour compte tenu des changements continuels qui se produisent dans l'environnement de sécurité. L'architecture de sécurité X.805 peut faciliter la gestion des politiques et des procédures de sécurité, des plans de réaction aux incidents et de récupération, ainsi que des architectures technologiques, en garantissant que les modifications apportées au programme de sécurité tiennent compte de chaque dimension de sécurité au niveau de chaque couche et de chaque plan de sécurité.

3 Concepts fondamentaux pour la protection: menaces, vulnérabilités et risques

Pour élaborer un cadre de sécurité, quel qu'il soit, il est très important d'avoir une idée claire des ressources nécessitant une protection, des menaces vis-à-vis desquelles ces ressources doivent être protégées, des vulnérabilités qu'elles présentent et du risque global qu'elles encourent compte tenu de ces menaces et vulnérabilités.

D'une manière générale, dans le domaine de la sécurité des TIC, les ressources nécessitant une protection peuvent être les suivantes:

- services de communications et services informatiques;
- informations et données, notamment les logiciels et les données concernant les services de sécurité; et
- équipements et installations.

Conformément à la Rec. UIT-T X.800, une *menace de sécurité* est une violation potentielle de la sécurité, par exemple:

- divulgation non autorisée d'informations;
- destruction ou modification non autorisée de données, d'équipements ou d'autres ressources;
- vol, suppression ou perte d'informations ou d'autres ressources;
- interruption ou déni de services; et
- usurpation de l'identité d'une entité autorisée.

Les menaces peuvent être *accidentelles* ou *délibérées* et peuvent être *actives* ou *passives*. Une menace accidentelle est une menace sans préméditation (par exemple dysfonctionnement d'un système ou d'un logiciel ou défaillance physique). Une menace délibérée est une menace dont la mise à exécution est un acte délibéré commis par une personne. (Lorsqu'une menace délibérée est mise à exécution, on parle alors d'*attaque*.) Une menace active est une menace résultant d'une modification d'état (par exemple altération de données ou destruction d'un équipement physique). Pour une menace passive, il n'y a pas de modification d'état (par exemple, l'écoute clandestine).

Une *vulnérabilité de sécurité* est un défaut ou une faiblesse susceptible d'être exploité pour violer un système ou les informations qu'il contient (X.800). Une vulnérabilité est susceptible d'engendrer la mise à l'exécution d'une menace.

Il existe quatre types de vulnérabilité: les vulnérabilités du *modèle des menaces* proviennent de la difficulté à prévoir les éventuelles menaces futures; les vulnérabilités de *conception et spécification* proviennent d'erreurs ou d'oublis dans la conception d'un système ou d'un protocole qui le rendent intrinsèquement vulnérable; les vulnérabilités d'*implémentation* proviennent d'erreurs au cours de l'implémentation d'un système ou d'un protocole; et les vulnérabilités d'*exploitation et de configuration* proviennent d'un mauvais usage d'options dans des implémentations ou de politiques de déploiement déficientes (par exemple la non-obligation d'utiliser le chiffrement dans un réseau Wi-Fi).

Un *risque de sécurité* est une mesure des effets négatifs qui peuvent se produire en cas d'exploitation d'une vulnérabilité de sécurité, autrement dit si une menace est mise à exécution. Le risque ne peut jamais être éliminé mais un objectif de la sécurité est de réduire le risque à un niveau acceptable. Pour cela, il faut comprendre les menaces et les vulnérabilités et appliquer des contremesures appropriées (à savoir des services et des mécanismes de sécurité).

Les menaces et les agents responsables de menaces varient alors que les vulnérabilités de sécurité existent pendant toute la durée de vie d'un système ou d'un protocole, sauf si des mesures spécifiques sont prises pour faire face aux vulnérabilités. Avec les protocoles normalisés, les risques de sécurité fondés sur les protocoles peuvent être très élevés et concerner le monde entier, d'où l'importance de comprendre et de détecter les vulnérabilités présentes dans les protocoles et de prendre des mesures pour faire face aux vulnérabilités une fois qu'elles ont été détectées.

Les organismes de normalisation ont à la fois une certaine responsabilité et une compétence unique pour ce qui est de faire face aux vulnérabilités de sécurité susceptibles d'être présentes dans des spécifications d'architectures, de cadres, de protocoles, etc. Même avec une bonne connaissance des risques, des vulnérabilités et des menaces associés aux réseaux informatiques et aux réseaux de télécommunications, il est impossible d'obtenir une sécurité correcte si on n'applique pas systématiquement les politiques de sécurité en vigueur, qui doivent être examinées et mises à jour régulièrement. Il faut aussi prévoir correctement la gestion de la sécurité et la prise en charge des incidents, par exemple déterminer les responsabilités et les mesures à prendre concernant la prévention des incidents de sécurité et la réaction aux incidents de sécurité (dispositions, contrôles, contre-mesures, garde-fou ou mesures à mettre en œuvre). L'UIT-T élabore actuellement de nouvelles Recommandations portant sur ces aspects de gestion de la sécurité.

4 Exigences de sécurité pour les réseaux de télécommunication

Le présent paragraphe contient des considérations de base sur la nécessité de fonctionnalités de sécurité et sur leurs caractéristiques du point de vue des utilisateurs, y compris les opérateurs de réseaux de télécommunication. Ces considérations découlent des exigences exprimées par diverses parties présentes sur le marché des télécommunications. Elles s'appuient principalement sur la Rec. UIT-T E.408 relative aux *prescriptions de sécurité des réseaux de télécommunication*. Cette Recommandation donne un aperçu général des prescriptions de sécurité et définit un cadre qui identifie les menaces de sécurité dans les réseaux de télécommunication en général (fixes ou mobiles; voix et données) et qui indique comment planifier des contre-mesures afin de limiter les risques découlant de ces menaces.

Elle a un caractère générique et n'indique pas ou ne tient pas compte d'exigences correspondant à des réseaux particuliers.

Elle ne définit pas de nouveaux services de sécurité mais utilise les services de sécurité existants définis dans d'autres Recommandations de l'UIT-T et dans des normes élaborées par d'autres organismes.

L'implémentation des prescriptions énoncées favorisera la coopération internationale dans les domaines ci-après concernant la sécurité des réseaux de télécommunication:

- partage et diffusion des informations;
- coordination en cas d'incident et réaction en cas de crise;
- recrutement et formation de professionnels de la sécurité;
- coordination de l'application des règlements;
- protection des infrastructures et services critiques;
- élaboration d'une législation appropriée.

Pour faciliter cette coopération, il est essentiel d'appliquer à l'échelle nationale les prescriptions concernant les composants nationaux du réseau.

4.1 Justification

Différentes entités ont besoin d'un cadre de sécurité de réseau générique pour les télécommunications internationales:

- *Les clients/abonnés* veulent que le réseau et les services offerts soient fiables et que les services soient disponibles (notamment les services d'urgence) en cas de catastrophes majeures (y compris les actes civils violents).

- *La communauté/les autorités publiques* exigent que la sécurité fasse l'objet de directives et de lois, afin de garantir la disponibilité des services, une concurrence loyale et la protection du respect de la vie privée.

- *Les opérateurs de réseau/fournisseurs de service* ont eux-mêmes besoin de sécurité pour sauvegarder leurs intérêts opérationnels et commerciaux et pour satisfaire à leurs obligations vis-à-vis des clients et du grand public, au niveau national comme au niveau international.

Les exigences de sécurité pour les réseaux de télécommunication devraient de préférence s'appuyer sur des normes de sécurité adoptées à l'échelle internationale car il vaut mieux réutiliser des normes plutôt que d'en créer de nouvelles. La mise en œuvre et l'utilisation de services et de mécanismes de sécurité peuvent s'avérer relativement onéreuses par rapport à la valeur des transactions protégées. Il est donc important de pouvoir personnaliser la sécurité offerte en fonction des services à protéger. Pour cela, il convient d'offrir les services et mécanismes de sécurité sous une forme qui permette de procéder à cette personnalisation. En raison du grand nombre de combinaisons possibles des fonctions de sécurité, il est souhaitable de disposer de *profils de sécurité* qui couvrent une grande variété de réseaux et services de télécommunication.

La normalisation facilite la *réutilisation de solutions et de produits*, ce qui signifie que la sécurité peut être mise en œuvre plus rapidement et à un moindre coût.

Les solutions normalisées présentent aussi de gros avantages pour les fabricants et les utilisateurs des systèmes: réalisation d'économies d'échelle lors de l'élaboration des produits et interfonctionnement des composants dans les réseaux de télécommunication du point de vue de la sécurité.

Il est nécessaire de mettre en place des services et des mécanismes de sécurité pour protéger les réseaux de télécommunication contre les attaques malveillantes telles que le déni de service, l'écoute clandestine, la mystification, l'altération des messages (modification, retard, suppression, insertion, relecture, réacheminement, déroutement ou réordonnancement de messages), la répudiation ou la falsification. La protection comprend la prévention et la détection des attaques et le retour à la normale après une attaque ainsi que la gestion des informations liées à la sécurité. Elle doit aussi comprendre des mesures visant à empêcher les interruptions de service dues à des événements naturels (météorologiques, etc.) ou à des attaques malveillantes (actes violents). Des dispositions doivent être prises pour permettre l'écoute et la surveillance lorsque celles-ci sont dûment autorisées par les autorités judiciaires.

4.2 Objectifs généraux de sécurité pour les réseaux de télécommunication

Le présent paragraphe décrit le but ultime des mesures de sécurité prises dans les réseaux de télécommunication et porte sur le résultat que les exigences de sécurité permettent d'obtenir et non pas sur la façon d'obtenir ce résultat.

Les objectifs de sécurité pour les réseaux de télécommunication sont les suivants:

a) seuls les utilisateurs autorisés devraient pouvoir accéder aux réseaux de télécommunication et les utiliser;

b) les utilisateurs autorisés devraient pouvoir accéder aux ressources pour lesquelles ils disposent d'autorisations d'accès et opérer sur ces ressources;

c) les réseaux de télécommunication devraient offrir le niveau de respect de la vie privée fixé par les politiques de sécurité qui leur sont applicables;

d) tous les utilisateurs devraient être tenus responsables de leurs actions et uniquement de leurs actions dans les réseaux de télécommunication;

e) afin d'en garantir la disponibilité, les réseaux de télécommunication devraient être protégés contre les accès et les opérations non sollicités;

f) il devrait être possible d'extraire des informations relatives à la sécurité à partir des réseaux de télécommunication (mais seuls les utilisateurs autorisés devraient pouvoir extraire ces informations);

g) lorsque des violations de la sécurité sont détectées, elles devraient être prises en charge de façon contrôlée conformément à un plan prédéfini de manière à minimaliser les dommages potentiels;

h) en cas de détection d'une atteinte à la sécurité, il devrait être possible de rétablir les niveaux de sécurité normaux;

i) l'architecture de sécurité des réseaux de télécommunication devrait offrir une certaine souplesse afin de prendre en charge différentes politiques de sécurité, par exemple différents niveaux de robustesse concernant les mécanismes de sécurité.

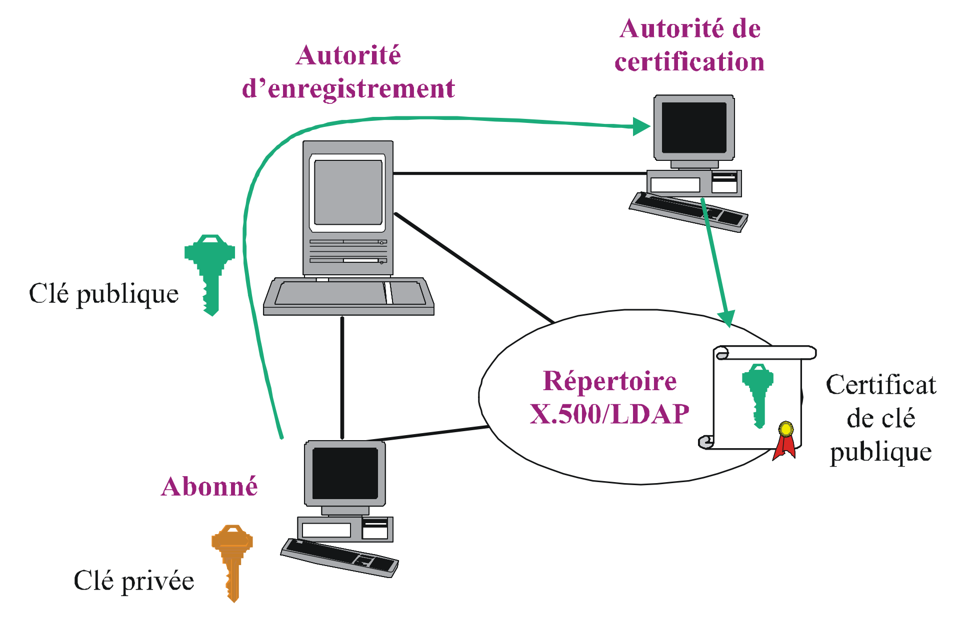
L'expression "accéder à des ressources" est entendue non seulement comme la possibilité d'exécuter des fonctions mais également de lire des informations.

On peut montrer que les cinq premiers objectifs de sécurité précités pour les réseaux de télécommunication seront remplis lorsque les mesures de sécurité suivantes sont mises en œuvre:

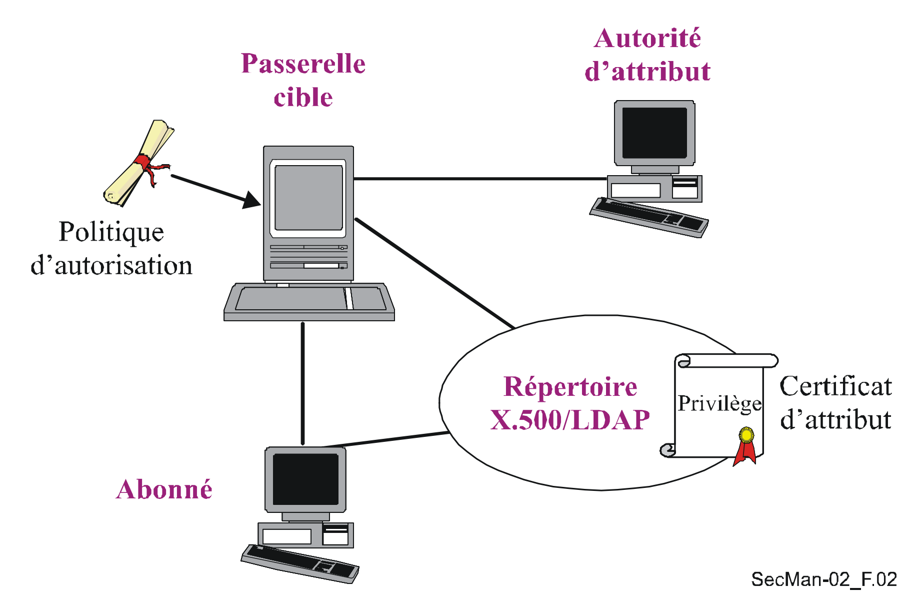
- la confidentialité;
- l'intégrité des données (l'intégrité des programmes système est certainement aussi requise);
- la responsabilité, y compris l'authentification, la non-répudiation et le contrôle d'accès;
- la disponibilité.

5 Infrastructures de clé publique et de gestion de privilège

La Rec. UIT-T X.509 (*L'annuaire: cadre général des certificats de clé publique et d'attribut*) définit une infrastructure de clé publique (PKI, *public key infrastructure*) normalisée en vue d'une authentification forte, fondée sur des certificats de clé publique et des autorités de certification. L'infrastructure PKI prend en charge la gestion de clés publiques pour assurer les services d'authentification, de chiffrement, d'intégrité et de non-répudiation. La technologie fondamentale d'une infrastructure PKI est la cryptographie à clé publique, qui est décrite ci-après. En plus de la définition d'un cadre d'authentification pour l'infrastructure PKI, la Rec. UIT-T X.509 définit aussi une infrastructure de gestion de privilège (PMI, *privilege management infrastructure*), qui sert à vérifier les droits et privilèges des utilisateurs dans le contexte d'une autorisation forte, fondée sur des certificats d'attribut et des autorités d'attribut. Les composants des infrastructures PKI et PMI sont illustrés sur la Figure 5-1.



a) Composants d'une infrastructure de clé publique



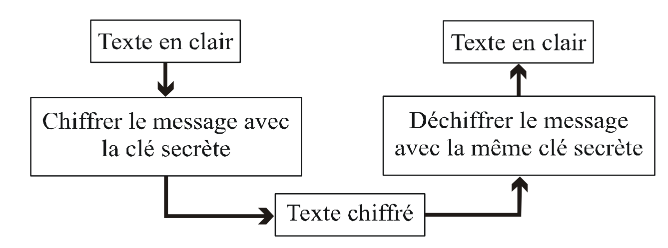
b) Composants d'une infrastructure de gestion de privilège

Figure 5-1 – Composants des infrastructures PKI et PMI

5.1 Cryptographie à clé secrète et cryptographie à clé publique

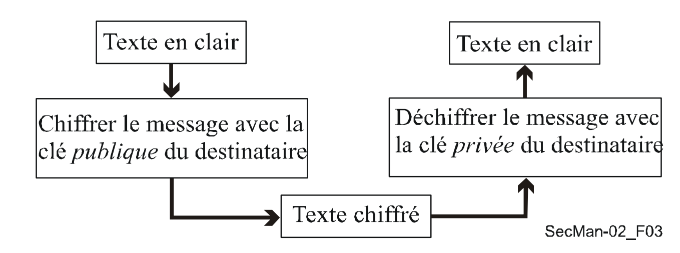
Dans un système de cryptographie *symétrique* (ou *à clé secrète*), on utilise la même clé pour le chiffrement et pour le déchiffrement, comme illustré sur la Figure 5-2a). Il faut donc faire en sorte que les individus puissent partager une clé secrète unique. La clé doit être distribuée aux individus par des moyens sécurisés, car la connaissance de la clé de chiffrement implique la connaissance de la clé de déchiffrement et inversement.

Un système de cryptographie *asymétrique* (ou à *clé publique*) fait intervenir deux clés, comme illustré sur la Figure 5-2b) – une clé publique et une clé privée. La clé publique peut être distribuée largement alors que la clé privée doit toujours être gardée secrète. La clé privée est généralement conservée sur une carte à puce ou sur un jeton. La clé publique est produite à partir de la clé privée et, bien que ces clés soient liées mathématiquement, il est impossible d'inverser le processus afin de déduire la clé privée de la clé publique. Pour envoyer à un destinataire des données confidentielles en toute sécurité en utilisant le chiffrement à clé publique, l'expéditeur chiffre les données avec la clé publique du destinataire et le destinataire les déchiffre avec sa clé privée correspondante. On peut aussi utiliser le chiffrement à clé publique pour appliquer une signature numérique à des données, le but étant de confirmer qu'un document ou un message provient bien de la personne qui déclare être l'expéditeur (ou l'auteur). La signature numérique est en réalité un résumé des données qui est produit au moyen de la clé privée du signataire et ajouté au document ou au message. Le destinataire utilise la clé publique du signataire pour confirmer la validité de la signature numérique. (NOTE – Certains systèmes à clé publique utilisent deux paires de clés publique/privée, l'une pour le chiffrement/déchiffrement, l'autre pour l'établissement/vérification de la signature numérique.)



– Les deux parties partagent une même clé secrète
– Problème: il est difficile d'échanger des clés dans un secret complet et ce type de chiffrement est difficilement applicable à une large communauté d'utilisateurs
– Exemple le plus connu: DES (norme de chiffrement des données)

a) Chiffrement à clé secrète (symétrique)



– Chaque participant a:
  – une clé privée qu'il ne partage avec personne d'autre
  – une clé publique que tout le monde connaît
– Problème: plus lent que le chiffrement à clé secrète
– Exemple le plus connu: RSA

b) Chiffrement à clé publique (asymétrique)

Figure 5-2 – Illustration des processus de chiffrement symétrique (ou à clé secrète) et asymétrique (ou à clé publique) et mise en évidence des particularités

Avec le chiffrement symétrique, chaque paire d'utilisateurs doit avoir une paire de clés différente et ces clés doivent être distribuées et conservées en toute sécurité. En revanche, avec le chiffrement asymétrique, les clés de chiffrement publiques peuvent être publiées dans un annuaire et chacun peut utiliser la même clé de chiffrement (publique) pour envoyer des données à un utilisateur donné. Ainsi, le chiffrement asymétrique est beaucoup plus facilement applicable à une large communauté que le chiffrement symétrique. Toutefois, le chiffrement asymétrique nécessite de très longs calculs, il est donc inefficace de chiffrer des messages entiers au moyen du chiffrement asymétrique. Dans la pratique, le chiffrement asymétrique est généralement utilisé pour échanger des clés symétriques qui

sont ensuite utilisées pour chiffrer le corps du message au moyen d'un algorithme symétrique plus efficace sur le plan des calculs. Lorsqu'une signature numérique est requise, le message est haché au moyen d'une fonction de hachage unidirectionnelle sécurisée telle que SHA1 ou MD5 et la valeur de hachage résultante codée sur 160 ou 128 bits est soumise à un chiffrement asymétrique au moyen de la clé privée de l'expéditeur puis jointe au message.

Il convient de noter que, quel que soit le mode de chiffrement (symétrique ou asymétrique), il est impossible d'acheminer des messages entièrement chiffrés à leurs destinataires car les nœuds intermédiaires ne pourraient pas déterminer l'adresse du destinataire. Par conséquent, les en-têtes de message ne doivent généralement pas être chiffrés.

La sécurité de fonctionnement d'un système à clé publique dépend fortement de la validité des clés publiques. Les clés publiques sont normalement publiées sous la forme de certificats numériques qui sont conservés dans un répertoire X.500. Un certificat contient non seulement la clé de chiffrement publique et, le cas échéant, la clé de vérification de la signature pour un individu, mais aussi d'autres informations, dont la validité du certificat. Les certificats qui ont été révoqués pour une raison ou pour une autre sont normalement inscrits sur une liste de révocation de certificats (CRL, *certificate revocation list*) figurant dans le répertoire. Avant d'utiliser des clés publiques, on vérifie normalement la liste CRL pour s'assurer de leur validité.

5.2 Certificats de clé publique

Un certificat de clé publique (parfois appelé "certificat numérique") est un moyen permettant de valider le propriétaire d'une paire de clés asymétriques. Un certificat de clé publique rattache fortement une clé publique au nom de son propriétaire et il est signé numériquement par l'autorité de confiance attestant ce rattachement. Cette autorité de confiance est appelée autorité de certification (CA, *certification authority*). Le format normalisé admis sur le plan international pour les certificats de clé publique est défini dans la Rec. UIT-T X.509. Brièvement, un certificat de clé publique X.509 comprend une clé publique, un identificateur de l'algorithme asymétrique avec lequel la clé doit être utilisée, le nom du propriétaire de la paire de clés, le nom de l'autorité de certification attestant cette propriété, le numéro de série et la période de validité du certificat, le numéro de la version X.509 à laquelle ce certificat est conforme et un ensemble facultatif de champs d'extension contenant des informations sur la politique de certification de l'autorité de certification. Le certificat entier est alors signé numériquement au moyen de la clé privée de l'autorité de certification. Un certificat X.509 peut être publié largement, par exemple sur un site web, dans un annuaire LDAP ou sur la carte de visite électronique (Vcard) attachée aux messages électroniques. La signature de l'autorité de certification garantit que le contenu du certificat ne peut pas être modifié sans que cela ne soit détecté.

Pour pouvoir confirmer la validité du certificat de clé publique d'un utilisateur, nous avons besoin de pouvoir accéder à la clé publique valable de l'autorité de certification qui a établi ce certificat, afin de vérifier la signature de l'autorité de certification sur ce certificat. La clé publique d'une autorité de certification peut être certifiée par une autre autorité de certification (supérieure), la validation des clés publiques pouvant alors faire intervenir une chaîne de certificats. Au bout du compte, cette chaîne doit avoir une fin, qui correspond généralement au certificat de l'autorité de certification qui constitue notre "racine de confiance". Les clés publiques d'autorité de certification racine sont distribuées sous la forme de certificats autosignés (dans lesquels les autorités de certification racines attestent qu'il s'agit de leur propre clé publique). La signature nous permet alors de valider le fait que la clé et le nom de l'autorité de certification n'ont pas été altérés depuis la création du certificat. Toutefois, nous ne pouvons pas prendre pour argent comptant le nom de l'autorité de certification figurant dans un certificat autosigné, car c'est l'autorité de certification qui a inséré le nom dans le certificat. Il est donc essentiel dans une infrastructure de clé publique que les clés publiques d'autorité de certification racine (sous forme de certificats autosignés) soient distribuées de manière sécurisée, afin que nous puissions être certains qu'une clé publique appartient réellement à l'autorité de certification racine dont le nom figure dans le certificat autosigné. Sans cela, nous ne pouvons pas être sûrs que l'identité de l'autorité de certification racine n'est pas usurpée.

5.3 Infrastructures de clé publique

L'infrastructure PKI est principalement destinée à émettre et gérer les certificats de clé publique, y compris les certificats autosignés d'autorité de certification racine. La gestion de clés comprend la création de paires de clés, la création de certificats de clé publique, la révocation de certificats de clé publique (par exemple si la clé privée d'un utilisateur a été compromise), le stockage et l'archivage des clés et des certificats et leur destruction une fois qu'ils sont arrivés au terme de leur vie. Chaque autorité de certification suit un ensemble de politiques et la Rec. UIT-T X.509 définit des mécanismes permettant de distribuer certaines de ces informations de politique dans les champs d'extension des certificats X.509 émis par les autorités de certification. Les règles et procédures politiques suivies par une autorité de certification sont généralement définies dans une politique de certificat (CP, *certificate policy*) et dans une déclaration de pratique de certification (CPS, *certification practice statement*), qui sont des documents publiés par l'autorité de certification. Ces documents constituent une base commune nous permettant d'évaluer la confiance que nous pouvons avoir concernant les certificats de clé publique émis par les autorités de certification, à la fois sur le plan international et d'un secteur à l'autre. Ils donnent aussi le (une partie du) cadre juridique nécessaire à l'établissement d'une confiance interorganisations et à la spécification de restrictions quant à l'utilisation des certificats émis.

Il est à noter que, dans le cas de l'authentification fondée sur des certificats de clé publique, les points d'extrémité sont tenus de fournir des signatures numériques établies au moyen de la valeur de la clé privée associée. L'échange de certificats de clé publique seuls n'offre pas de protection contre les attaques de l'intercepteur (*man-in-the-middle*).

5.4 Infrastructure de gestion de privilège

Les premières versions de la Rec. UIT-T X.509 (1988, 1993 et 1997) (*L'annuaire: cadre d'authentification*) spécifiaient les éléments de base nécessaires pour les infrastructures de clé publique et définissaient notamment les certificats de clé publique. La Rec. UIT-T X.509 révisée qui a été approuvée en 2000 contient des précisions sur les certificats d'attribut et définit un cadre pour l'infrastructure de gestion de privilège (PMI, *privilege management infrastructure*). (Une infrastructure PMI gère les privilèges pour prendre en charge un service d'autorisation complet en relation avec une infrastructure PKI.) Les mécanismes définis permettent d'établir des privilèges d'accès pour les utilisateurs dans un environnement multifabricant et multi-application.

Les infrastructures PMI et PKI utilisent des concepts analogues, mais l'infrastructure PMI concerne l'autorisation tandis que l'infrastructure PKI concerne l'authentification. La Figure 5-1 et le Tableau 5-1 illustrent les analogies entre les deux infrastructures.

Tableau 5-1 – Comparaison des caractéristiques de l'infrastructure de gestion de privilège et de l'infrastructure de clé publique

Infrastructure de gestion de privilège	Infrastructure de clé publique
Source d'autorité (SoA)	Autorité de certification racine (point d'ancrage de confiance)
Autorité d'attribut (AA)	Autorité de certification
Certificat d'attribut	Certificat de clé publique
Liste de révocation de certificats d'attribut	Liste de révocation de certificats
Liste de révocation d'autorités pour l'infrastructure PMI	Liste de révocation d'autorités pour l'infrastructure PKI

L'attribution de privilèges aux utilisateurs vise à faire en sorte que les utilisateurs suivent une politique de sécurité prescrite établie par la source d'autorité. Les informations relatives à cette politique sont rattachées au nom d'utilisateur dans le certificat d'attribut et comprennent un certain nombre d'éléments illustrés sur la Figure 5-3.

Version
Détenteur
Emetteur
Signature (identificateur d'algorithme)
Numéro de série de certificat
Durée de validité
Attributs
Identificateur unique de l'émetteur
Extensions

Figure 5-3 – Structure d'un certificat d'attribut X.509

Le modèle de contrôle de l'infrastructure PMI défini dans la Rec. UIT-T X.509 est constitué de cinq composants: le déclarant de privilège, le vérificateur de privilège, la méthode objet[1], la politique de privilège et les variables d'environnement (voir la Figure 5-4). Les procédés décrits permettent au vérificateur de privilège de contrôler l'accès du déclarant de privilège à la méthode objet, conformément à la politique de privilège.

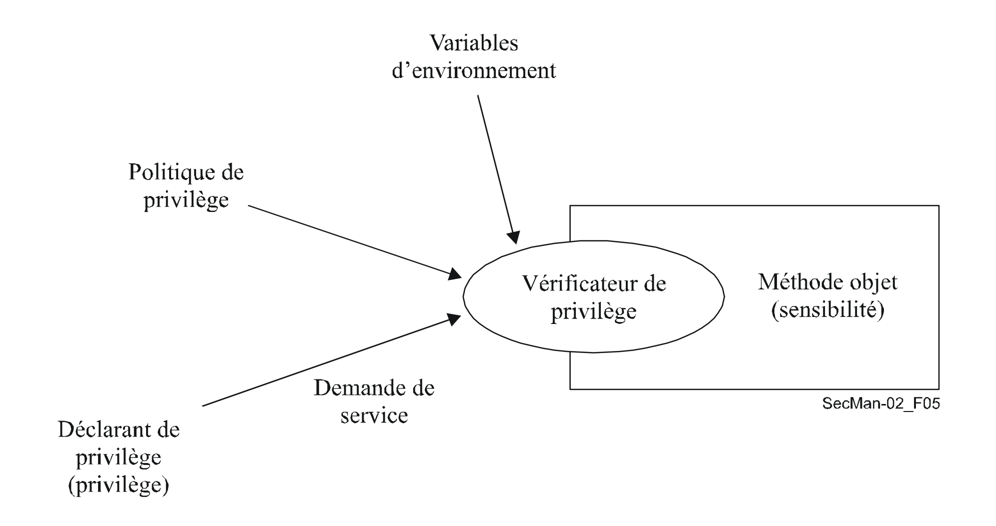


Figure 5-4 – Modèle de contrôle de l'infrastructure PMI (Rec. UIT-T X.509)

Pour certaines implémentations, il peut être nécessaire de déléguer un privilège. Le modèle de délégation de l'architecture PMI défini dans la Rec. UIT-T X.509 est constitué de quatre composants: le vérificateur de privilège, la source d'autorité, d'autres autorités d'attribut et le déclarant de privilège (voir la Figure 5-5).

[1] Une méthode objet est définie comme une action qui peut être invoquée sur une ressource (par exemple un système de fichiers peut avoir des méthodes objets lecture, écriture et exécution).

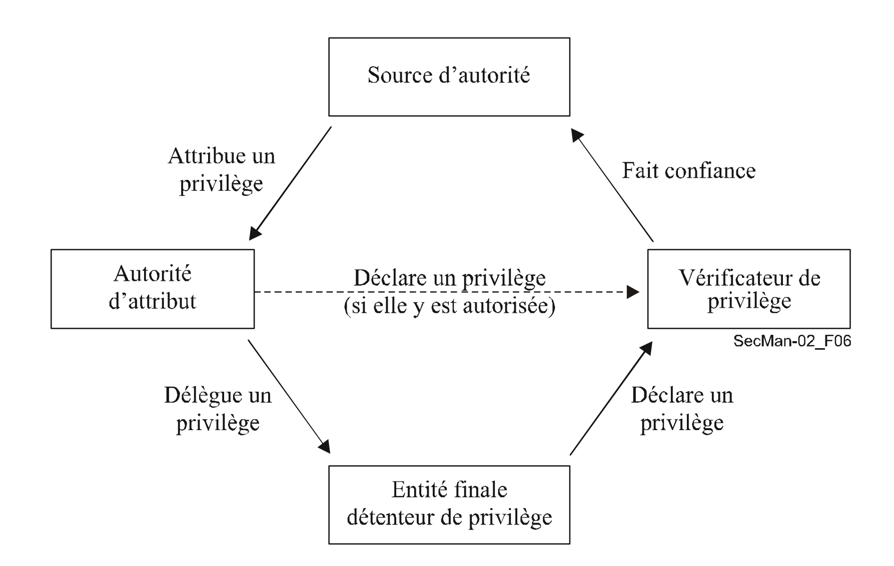


Figure 5-5 – Modèle de délégation de l'infrastructure PMI (Rec. UIT-T X.509)

Dans les implémentations récentes de systèmes d'autorisation fondées sur le modèle du contrôle d'accès à base de rôle (RBAC, *role-based access control*), on considère qu'un rôle est attribué à l'utilisateur. La politique d'autorisation associe un ensemble de permissions à un rôle. Lorsque l'utilisateur accède à une ressource, son rôle est d'abord vérifié avant qu'il ne puisse invoquer des actions. Le système d'ordonnances électroniques décrit au § 6.5.2 est un exemple d'utilisation d'un système RBAC.

6 Applications

Les applications dont il est question ici appartiennent à deux catégories distinctes. La première catégorie correspond aux applications d'utilisateur final. Elle comprend notamment la téléphonie IP (VoIP, *voice-over-IP*), pour laquelle l'architecture de réseau et les composants utilisés pour offrir cette application d'utilisateur final sont décrits. Des problèmes de sécurité et des solutions sont examinés dans les trois plans de sécurité dans le cas des applications multimédias et de la VoIP en particulier. Le système IPCablecom, qui offre des services IP en temps réel sur un réseau de transmission par câble, et la transmission de télécopie sont deux autres applications d'utilisateur final traitées ici. Parmi les applications qui ne sont pas propres au secteur des télécommunications et qui sont examinées ici, figure la télésanté et notamment un système d'ordonnances électroniques. La seconde catégorie correspond aux applications de gestion de réseau, dans lesquelles la sécurité est un élément important à prendre en considération afin que la qualité et l'intégrité des services offerts par les fournisseurs puissent être respectées. Il est donc impératif de mettre en place un système approprié de privilèges et d'autorisations pour l'exécution des activités de gestion.

6.1 Téléphonie IP utilisant des systèmes H.323

La téléphonie IP, également appelée voix sur IP (VoIP, *voice-over-IP*), désigne la fourniture de services traditionnellement offerts sur le réseau téléphonique public commuté (RTPC) (à commutation de circuit) sur un réseau utilisant le protocole IP (sur lequel l'Internet est fondé). Ces services comprennent avant tout la téléphonie, mais aussi d'autres formes de média, y compris la vidéo et les données (par exemple le partage d'applications et la fonctionnalité de tableau blanc électronique). La téléphonie IP inclut aussi les services complémentaires associés tels que les conférences (par pont de conférence), le renvoi d'appel, l'appel en instance, les lignes multiples, la déviation d'appel, la mise en garde et l'interception d'appel, la consultation et la fonction suis-moi, et bien d'autres services de réseau intelligent, ainsi que les données dans la bande vocale dans certains cas. La téléphonie sur Internet est un cas particulier de VoIP, dans lequel le trafic téléphonique est acheminé sur l'Internet public.

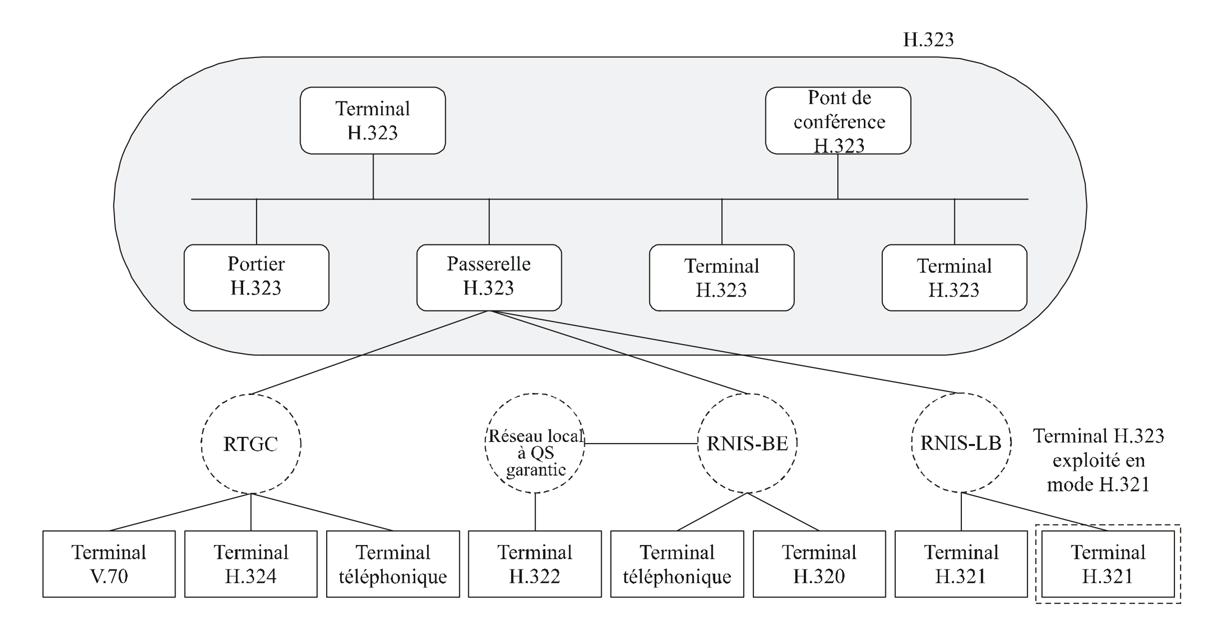
H.323 est une Recommandation cadre de l'UIT-T qui jette les bases des communications audio, vidéo et de données sur les réseaux à commutation par paquets, y compris l'Internet, les réseaux locaux (LAN, *local-area network*) et les réseaux régionaux (WAN, *wide-area network*), qui n'offrent pas de qualité de service garantie. Ces réseaux, qui sont actuellement les principaux réseaux utilisés dans les entreprises, emploient les technologies de réseau suivantes: TCP/IP à commutation par paquets et IPX sur Ethernet, Fast Ethernet et Token Ring. Les produits et applications multimédias issus de différents fabricants mais conformes à la Rec. UIT-T H.323 peuvent interfonctionner, ce qui permet aux utilisateurs de communiquer sans avoir à se soucier de la compatibilité. Le protocole H.323 a été le premier protocole de téléphonie IP à être défini et il est considéré comme la pierre angulaire pour les produits fondés sur la téléphonie IP destinés aux applications de divertissement ou professionnelles des particuliers, des entreprises et des fournisseurs de services. Les principales Recommandations concernant le système H.323 sont les suivantes:

- H.323 – document "cadre" qui décrit l'utilisation des Recommandations UIT-T H.225.0 et H.245 et d'autres documents connexes pour la fourniture de services de conférence multimédias en mode paquet.
- H.225.0 – document qui décrit trois protocoles de signalisation (RAS, signalisation d'appel et "Annexe G").
- H.245 – protocole de commande multimédia (commun aux Recommandations UIT-T H.310, H.323 et H.324).
- H.235.x – sécurité dans les systèmes de type H.323.
- H.246 – interfonctionnement avec le RTPC.
- H.450.x – services complémentaires.
- H.460.x – diverses extensions du protocole H.323.
- H.501 – protocole de gestion de la mobilité et communications intra et interdomaines.
- H.510 – mobilité d'utilisateur, de terminal et de service.
- H.530 – spécification de la sécurité pour la Rec. UIT-T H.510.

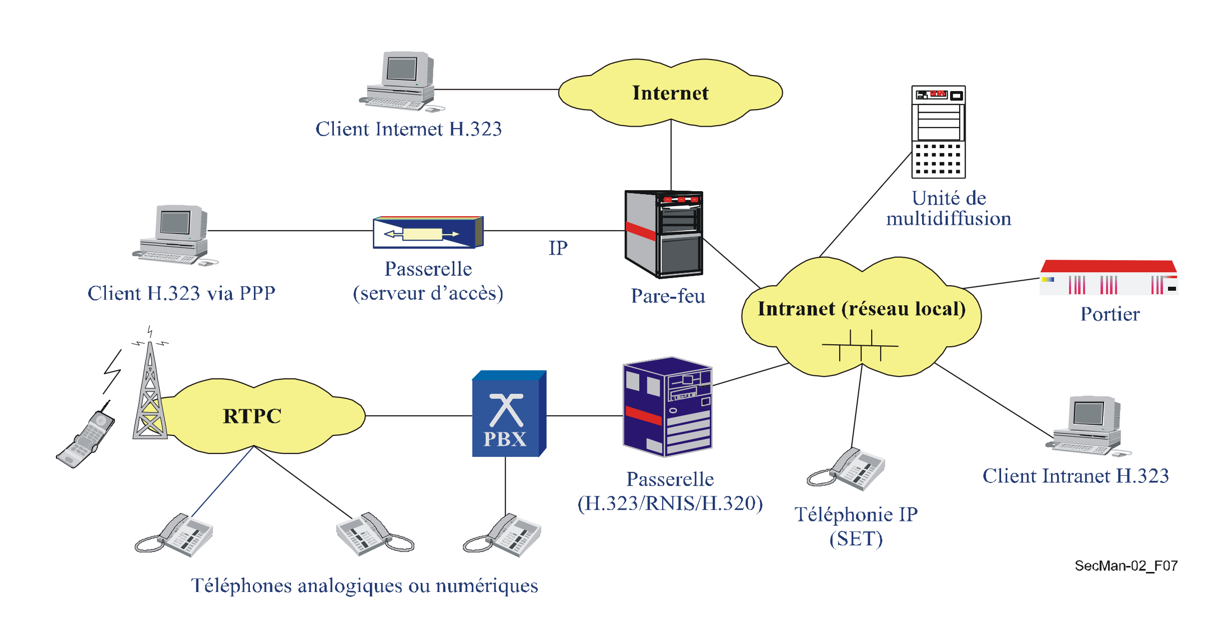
L'UIT-T a approuvé la première version de la Rec. UIT-T H.323 en 1996. La version 2 a été approuvée en janvier 1998 et la version actuelle (version 6) a été approuvée en 2006. Cette norme au domaine d'application vaste inclut les dispositifs autonomes et les ordinateurs personnels intégrés ainsi que les conférences point à point et multipoint. Elle traite de la commande d'appel, de la gestion multimédia et de la gestion de largeur de bande ainsi que des interfaces entre différents réseaux.

La Rec. UIT-T H.323 fait partie d'une série de normes de communications permettant d'offrir des services de visioconférence dans des réseaux divers. Connue sous l'appellation H.32x, cette série de Recommandations comprend les Recommandations UIT-T H.320 et H.324, qui portent respectivement sur les communications dans le RNIS et dans le RTPC. Le présent ouvrage donne un aperçu de la norme H.323, de ses avantages, de son architecture et de ses applications.

La Rec. UIT-T H.323 définit quatre principaux composants pour un système de communication fondé sur des réseaux: terminaux, passerelles, portiers et ponts de conférence. En outre, des éléments frontières ou homologues sont également possibles. Ces éléments apparaissent sur la Figure 6-1.



a) Système H.323 et ses composants [Packetizer]



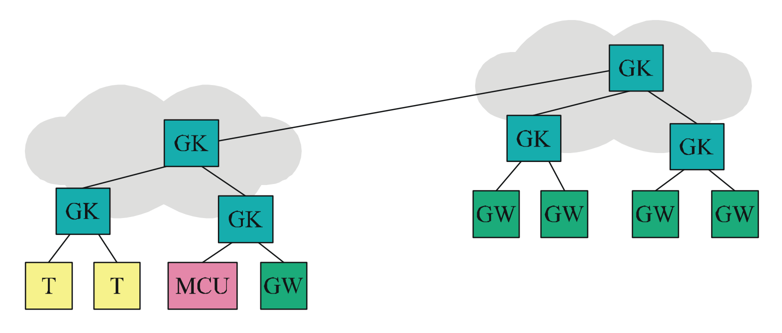
b) Scénarios de déploiement H.323 [Euchner]

Figure 6-1 – Système H.323: composants et scénarios de déploiement

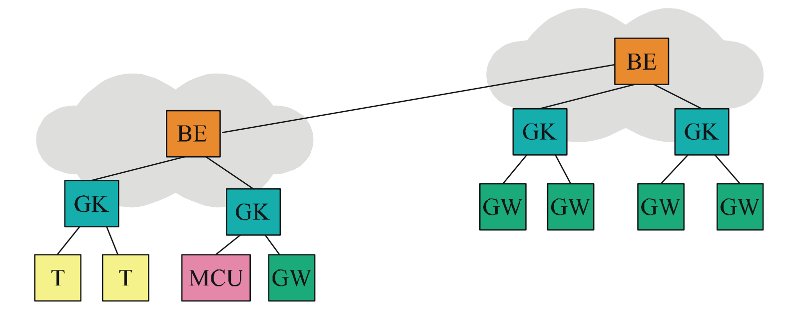
Les *terminaux (T)* sont les points d'extrémité client sur le réseau dorsal IP qui prennent en charge des communications bidirectionnelles. Les terminaux H.323 doivent prendre en charge les communications téléphoniques et peuvent prendre en charge des codecs vidéo, des protocoles de conférence de données T.120 et des capacités de pont de conférence. Ce sont par exemple des téléphones IP, des visiophones, des dispositifs à réponse vocale interactive, des systèmes de messagerie vocale, des "logiciels de téléphonie sur ordinateur" (par exemple NetMeeting™).

La *passerelle* (*GW*, *gateway*) offre de nombreux services, le plus courant étant une fonction de traduction entre les points d'extrémité H.323 et les autres types de terminaux. Cette fonction inclut la traduction entre formats de transmission (par exemple entre H.225.0 et H.221) et entre procédures de communication (par exemple entre H.245 et H.242). En outre, la passerelle assure également la traduction entre codecs audio et vidéo et procède à l'établissement et à la libération d'appel à la fois côté réseau à commutation par paquets et côté réseau à commutation de circuit.

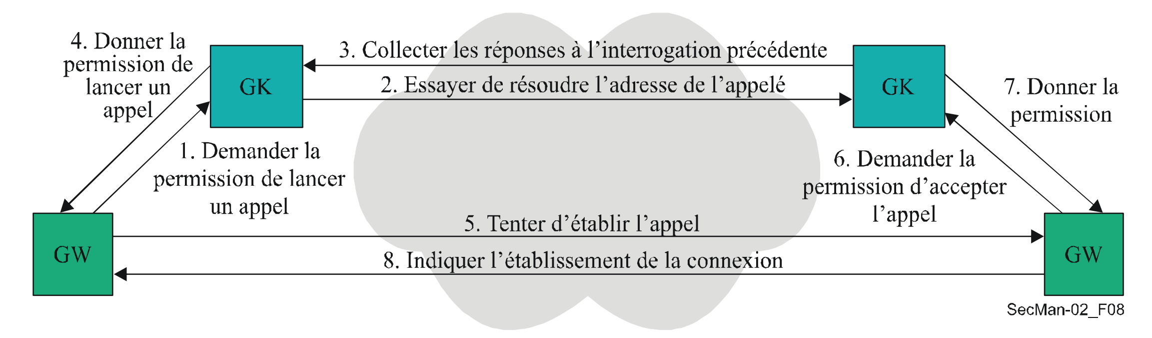
Le *portier* (*GK, gatekeeper*) est un composant important d'un réseau de type H.323. Il est le point central pour tous les appels à l'intérieur de sa zone et offre des services de commande d'appel aux points d'extrémité enregistrés. De nombreuses façons, le portier H.323 joue le rôle de commutateur virtuel, étant donné qu'il exécute le contrôle à l'admission, la résolution d'adresse et qu'il peut autoriser le lancement direct d'appels entre points d'extrémité ou qu'il peut faire transiter la signalisation d'appel par lui afin d'exécuter des fonctions telles que suis-moi/trouve-moi, renvoi d'appel sur occupation, etc. Les portiers sont associés à des *éléments frontières* (ou homologues) (*BE, border element*), qui sont chargés d'échanger des informations d'adressage et de participer à l'autorisation d'appel entre domaines administratifs (ou à l'intérieur d'un domaine administratif). Cette fonctionnalité assure également l'intercommunication entre différents réseaux ou "îlots" H.323. Pour cela, une série de messages est échangée, comme illustré sur la Figure 6-2.



a) Topologie avec le protocole RAS



b) Topologie avec le protocole de l'Annexe G/H.225.0



c) Flux d'appel de haut niveau

Légende: BE: élément frontière; GK: portier; GW: passerelle; MCU: pont de conférence; T: terminal; RAS: protocole d'enregistrement, admission et état

Figure 6-2 – Communications entre domaines administratifs

Le *pont de conférence* (*MCU, multipoint control unit*) prend en charge les conférences entre trois points d'extrémité ou plus. Selon la Rec. UIT-T H.323, un pont de conférence comprend un contrôleur multipoint obligatoire et zéro, un ou plusieurs processeurs multipoint. Le contrôleur multipoint gère la signalisation d'appel mais ne prend pas directement en charge les flux de médias. Cette prise en charge est assurée par les processeurs multipoint, qui mélangent, commutent et traitent les bits audio, vidéo et/ou de données. Les capacités du contrôleur multipoint et des processeurs multipoint peuvent se trouver dans un composant spécialisé ou faire partie d'autres composants H.323.

Les réseaux H.323 actuellement en service acheminent des milliards de minutes de trafic téléphonique et vidéo chaque mois; l'acheminement de la majeure partie du trafic de téléphonie IP se fait maintenant selon le protocole H.323. On estime actuellement que la téléphonie IP représente plus de 10 pour cent de toutes les minutes de communications téléphoniques internationales longue distance. Par ailleurs, le trafic vidéo H.323 augmente constamment. Ceci s'explique essentiellement par le fait que le protocole H.323 et ses implémentations sont bien définis et très modulables et répondent ainsi aux besoins des fournisseurs de services et des entreprises, les produits H.323 allant de piles et de puces à des téléphones mobiles et à des matériels de visioconférence.

Les systèmes H.323 assurent les fonctionnalités suivantes:

- Capacité de conférence téléphonique, vidéo et données.
- Communications entre divers types de terminaux, y compris les communications entre un ordinateur et un téléphone, entre deux télécopieurs, entre deux téléphones et les communications sur le web.
- Prise en charge de la télécopie T.38, du texte sur IP et des modems sur IP.
- De nombreux services complémentaires (renvoi d'appel, interception d'appel, etc.).
- Forte interopérabilité avec les autres systèmes H.32x, notamment H.320 (RNIS) et H.323M (systèmes hertziens mobiles 3GPP).
- Spécification de décomposition de passerelle média (via le protocole de commande de passerelle H.248).
- Prise en charge de la signalisation et de la sécurité des médias.
- Mobilité d'utilisateur, de terminal et de service.
- Prise en charge de la signalisation des services d'urgence.

Le protocole H.323 est par exemple utilisé pour le transit en masse par les opérateurs, notamment dans les réseaux dorsaux de téléphonie IP (comparables à des commutateurs de classe 4 pour le trafic téléphonique) et pour les services de carte d'appel. Dans les entreprises, le protocole H.323 est utilisé pour les autocommutateurs IP, les centres IP, les réseaux privés virtuels téléphoniques, les systèmes téléphonie et données intégrées, les téléphones Wi-Fi, l'implémentation de centres d'appel et les services de mobilité. A titre professionnel, les personnes l'utilisent largement pour les conférences téléphoniques (ou audio) et vidéo, pour la collaboration téléphonie/données/vidéo et pour le télé-enseignement. A titre privé, elles l'emploient notamment pour l'accès audiovisuel à large bande et pour les communications de PC à téléphone, de téléphone à PC ou de PC à PC; le protocole H.323 peut aussi être utilisé pour la diffusion d'informations et d'actualités personnalisées.

6.1.1 Problèmes de sécurité dans le domaine du multimédia et de la téléphonie IP

Comme tous les éléments d'un système H.323 peuvent être répartis géographiquement et que les réseaux IP sont ouverts, plusieurs menaces de sécurité peuvent surgir, comme l'illustre la Figure 6-3.

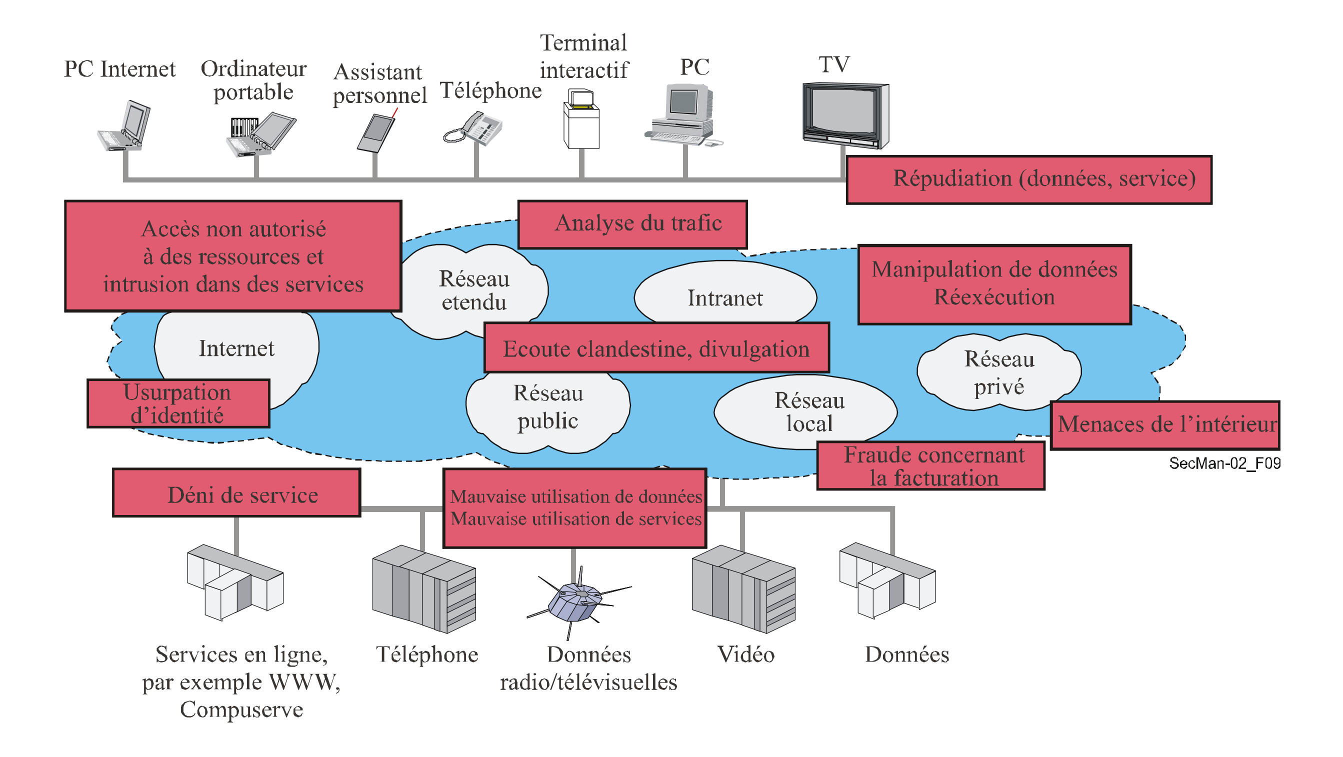


Figure 6-3 – Menaces de sécurité dans les communications multimédias

Les principaux problèmes de sécurité qui se posent dans le domaine des communications multimédias et de la téléphonie IP en général sont décrits en détail ci-dessous [Euchner]:

- Authentification d'utilisateur et de terminal: les fournisseurs de services de téléphonie IP ont besoin de savoir qui utilise leur service pour pouvoir comptabiliser et éventuellement facturer correctement l'utilisation du service. En vue de l'authentification, l'utilisateur et/ou le terminal doit d'abord s'identifier avec une certaine identité, puis prouver que l'identité déclarée est la véritable identité. Pour cela, il est généralement fait appel à des procédures d'authentification forte par chiffrement (par exemple mot de passe protégé ou signatures numériques X.509). De même, les utilisateurs peuvent souhaiter savoir qui sont leurs correspondants téléphoniques.

- Authentification de serveur: comme les utilisateurs de téléphonie IP communiquent généralement entre eux par le biais d'une certaine infrastructure de téléphonie IP faisant intervenir des serveurs (portiers, unités de multidiffusion, passerelles), ils souhaitent savoir s'ils sont reliés au serveur correct et/ou au fournisseur de services correct. Cet aspect concerne les utilisateurs fixes comme les utilisateurs mobiles.

- Menaces de sécurité lors de l'authentification d'utilisateur/de terminal et de serveur, telles que l'usurpation d'identité, l'attaque de l'intercepteur, la mystification d'adresse IP et le détournement de connexion.

- L'autorisation d'appel est le processus qui consiste à déterminer si l'utilisateur/le terminal est réellement autorisé à utiliser les ressources de service, par exemple une fonctionnalité de service (appel dans le RTPC, etc.) ou une ressource de réseau (qualité de service, largeur de bande, codec etc.). Le plus souvent, les fonctions d'authentification et d'autorisation sont rassemblées afin qu'une décision puisse être prise au niveau du contrôle d'accès. L'authentification et l'autorisation aident à contrecarrer les attaques de type usurpation d'identité, mauvaise utilisation et fraude, manipulation et déni de service.

- La protection de sécurité de la signalisation concerne la protection des protocoles de signalisation contre les manipulations et les mauvaises utilisations ainsi que la protection en termes de confidentialité et de respect de la vie privée. Les protocoles de signalisation sont généralement protégés par des moyens cryptographiques et font l'objet d'une protection d'intégrité et d'une protection contre les réexécutions. Il faut tout particulièrement veiller à ce que les facteurs de qualité critiques des communications en temps réel soient respectés et, pour cela, il faut utiliser des procédures courtes de prise de contact et des temps de transmission aller-retour courts afin d'éviter que la durée d'établissement d'une communication soit trop longue ou que la qualité téléphonique soit dégradée par suite de retards de paquets ou de gigue en raison d'un traitement de sécurité.
- La confidentialité téléphonique est assurée par le chiffrement des paquets téléphoniques, c'est-à-dire les charges utiles RTP, et par la contre-écoute des données téléphoniques surveillées. En général, les paquets de média (par exemple vidéo) d'applications multimédias sont également chiffrés. La protection renforcée des paquets de média comprend également l'authentification/la protection d'intégrité des charges utiles.
- La gestion de clés inclut non seulement toutes les tâches qui sont nécessaires pour que les parties puissent distribuer de manière sécurisée les informations relatives aux clés aux utilisateurs et aux serveurs, mais aussi les tâches liées à la mise à jour de clé en cas d'expiration ou aux clés perdues. La gestion de clés peut être exécutée en dehors de l'application de téléphonie IP (fourniture de mot de passe) ou peut être intégrée à la signalisation lorsque des profils de sécurité avec capacités de sécurité sont négociés dynamiquement et que des clés de session doivent être distribuées.
- La sécurité interdomaines se rapporte au problème découlant du fait que des systèmes appartenant à des environnements hétérogènes ont implémenté des fonctionnalités de sécurité différentes en raison de besoins différents, de politiques de sécurité différentes et de capacités de sécurité différentes. Il faut donc négocier dynamiquement des profils et des capacités de sécurité tels que des algorithmes de chiffrement et leurs paramètres. Cela devient notamment important lorsque des frontières entre domaines sont franchies et que des fournisseurs et des réseaux différents interviennent. En ce qui concerne les communications interdomaines, il est important, du point de vue de la sécurité, de pouvoir traverser les pare-feu sans encombre et de pouvoir faire face aux contraintes liées aux traducteurs d'adresse de réseau (NAT, *network address translation*).

La liste n'est pas complète mais il s'agit là de l'essentiel de la sécurité H.323. En pratique, toutefois, on peut se retrouver confronté à d'autres problèmes de sécurité qui sont considérés comme ne faisant pas partie du domaine d'application du protocole H.323 (par exemple problèmes liés à la politique de sécurité, à la sécurité de gestion de réseau, à l'implémentation de la sécurité, à la sécurité opérationnelle ou à la prise en charge des incidents de sécurité).

6.1.2 Aperçu des Recommandations de la sous-série H.235.x

La Rec. UIT-T H.235.0 définit le cadre de sécurité des systèmes multimédias H.323 et spécifie notamment les mécanismes et protocoles de sécurité. La Rec. UIT-T H.235 a été publiée pour la première fois en 1998 pour les systèmes H.323 de version 2. Depuis, elle a été étoffée: les mécanismes de sécurité offerts ont été renforcés, des algorithmes de sécurité plus sophistiqués ont été ajoutés (par exemple chiffrement AES très rapide et très sûr) et des profils de sécurité utiles et efficaces ont été élaborés pour certains scénarios d'utilisation et environnements. Les Recommandations UIT-T H.235.0 à H.235.9 de la version 4 constituent la série actuelle de Recommandations UIT-T définissant une sécurité modulable des systèmes H.323 aussi bien pour des petits groupes que pour des entreprises ou des opérateurs à grande échelle.

L'ancienne version 3 de la Rec. UIT-T H.235 a subi une importante restructuration de l'ensemble de ses parties et annexes et il en est résulté un ensemble complet de Recommandations autonomes de la sous-série H.235.x, la Rec. UIT-T H.235.0 définissant le "cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245)". Cette Recommandation donne un aperçu de la sous-série H.235.x et définit les procédures communes avec un texte de base.

En quelques mots, les Recommandations UIT-T de la série H.235.x assurent une protection cryptographique des protocoles de commande (RAS et signalisation d'appel H.225.0 et H.245) ainsi qu'une protection cryptographique des données de flux médias audio/vidéo. Au cours des diverses étapes de la signalisation H.323, la série H.235 offre des moyens permettant de négocier les services cryptographiques, les algorithmes de chiffrement et les capacités de sécurité souhaités et requis. Les fonctions de gestion de clés pour l'établissement de clés de session dynamiques sont entièrement intégrées aux procédures de prise de contact, ce qui permet de réduire la durée d'établissement d'appel. La gestion de clés H.235 prend en charge la configuration point à point "classique" mais aussi les configurations multipoint avec unités de multidiffusion (c'est-à-dire ponts de conférence) lorsque plusieurs terminaux multimédias communiquent dans un groupe.

La série H.235 utilise des techniques de sécurité optimisées particulières (cryptographie à courbe elliptique et chiffrement AES moderne par exemple) afin de respecter les contraintes strictes de qualité. Lorsque le chiffrement téléphonique est implémenté, on procède au chiffrement des charges utiles RTP dans la couche application. Cette façon de procéder est avantageuse; en effet, elle a peu d'incidence sur les points d'extrémité grâce à une interaction étroite avec le processeur de signaux numériques (DSP, *digital signal processor*) et les codecs de compression vocale et elle ne dépend pas d'une plate-forme de système d'exploitation particulière. Les outils de sécurité existants (par exemple paquetages et normes de sécurité Internet (IPSec, SSL/TLS)) qui sont disponibles et appropriés peuvent être (ré)utilisés dans le contexte de la série H.235.

La Figure 6-4 illustre le domaine d'application de la série H.235, qui contient des dispositions relatives à l'établissement d'appels (blocs H.225.0 et H.245) et de communications bidirectionnelles (chiffrement de charges utiles RTP contenant des signaux audio et/ou vidéo compressés). Les fonctionnalités comprennent des mécanismes pour l'authentification, l'intégrité, le respect de la vie privée et la non-répudiation. Les portiers doivent prendre en charge l'authentification en contrôlant l'admission au niveau des points d'extrémité et fournir des mécanismes de non-répudiation. La sécurité dans la couche de transport et dans les couches inférieures, fondées sur IP, sort du cadre des Recommandations UIT-T H.323 et H.235, mais elle est couramment implémentée au moyen des protocoles de sécurité IP (IPSec) de l'IETF et de sécurité dans la couche transport (TLS, *transport layer security*). D'une manière générale, le protocole IPSec ou TLS peut être utilisé pour assurer l'authentification et, facultativement, la confidentialité (c'est-à-dire le chiffrement) dans la couche IP quel que soit le protocole (d'application) qui est exécuté au-dessus et sans que ce protocole ne doive être mis à jour, seule la politique de sécurité à chaque extrémité doit être actualisée.

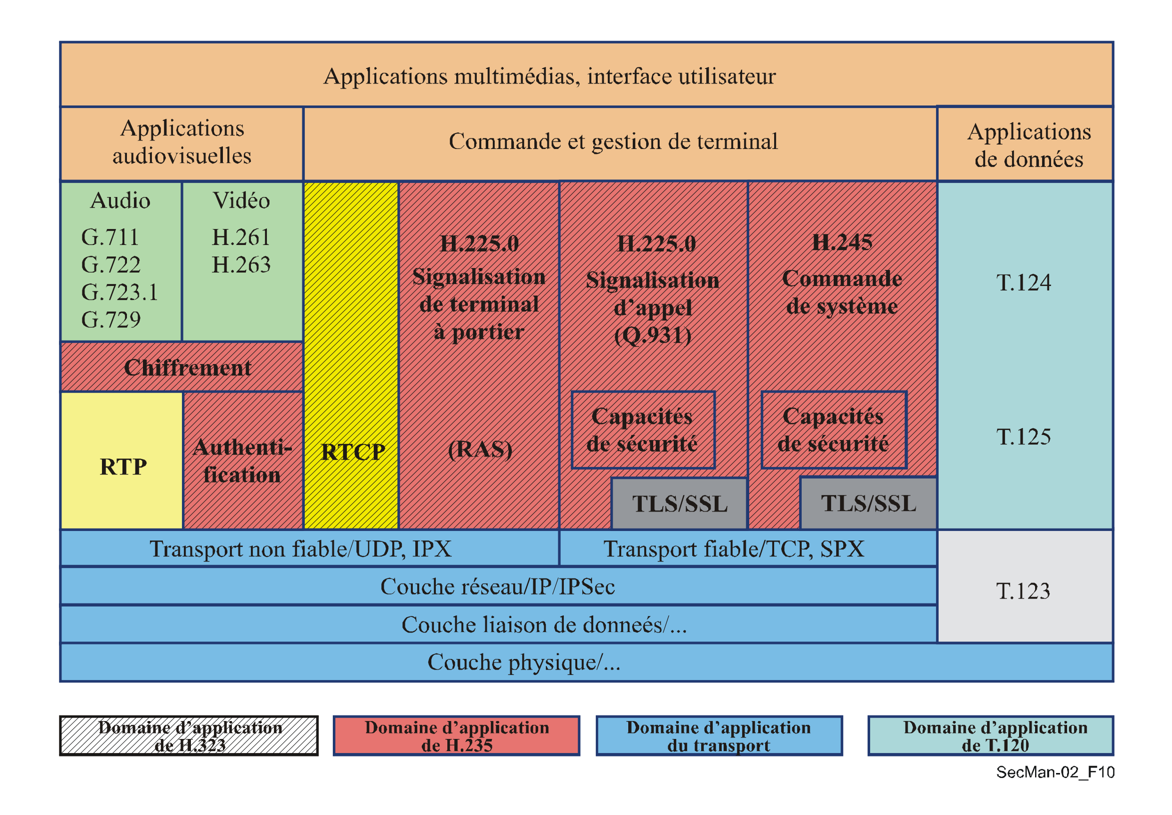


Figure 6-4 – Sécurité des systèmes H.323 offerte par la série H.235 [Euchner]

Les Recommandations UIT-T de la série H.235.x décrivent une large palette de mesures de sécurité applicables dans différents environnements cibles, par exemple les environnements intra/inter-entreprises et les environnements d'opérateurs. Suivant les hypothèses prises, par exemple en termes d'infrastructure de sécurité disponible, de capacités de terminal et de plates-formes (par exemple points d'extrémité simples ou points d'extrémité intelligents), les Recommandations UIT-T H.235.x offrent divers profils de sécurité personnalisés et interopérables propres à un scénario donné. Les profils de sécurité disponibles vont de simples profils à secret partagé avec mot de passe protégé (H.235.1 pour l'authentification et l'intégrité des messages de signalisation H.225.0) à des profils plus complexes avec signatures numériques et certificats PKI X.509 (H.235.2). Ainsi, il est possible de mettre en œuvre une protection bond par bond en utilisant les techniques les plus simples mais les moins modulables ou une protection de bout en bout en utilisant les techniques PKI modulables. La Rec. UIT-T H.235.3 est appelée profil de sécurité hybride car elle combine les procédures de sécurité symétriques de la Rec. UIT-T H.235.1 avec les signatures et certificats fondés sur l'infrastructure PKI de la Rec. UIT-T H.235.2, ce qui permet d'optimiser la performance et de raccourcir les temps d'établissement d'appel. La Rec. UIT-T H.235.3 offre en outre la possibilité d'implémenter facultativement des opérations nécessitant de nombreux calculs dans un processeur de sécurité fondé sur un proxy.

La Rec. UIT-T H.235.4, intitulée "Sécurité des appels à routage direct et des appels à routage sélectif", assouplit la nécessité stricte d'une architecture centrée sur un serveur et avec routage par portier et définit des mesures de sécurité visant à sécuriser un modèle d'homologue à homologue. Cette Recommandation définit des procédures de gestion de clé dans des environnements d'entreprise et dans des environnements interdomaines. La Rec. UIT-T H.235.4 couvre en particulier les scénarios dans lesquels le portier fonctionne en mode de routage direct ou dans lesquels le portier peut tout juste effectuer un routage sélectif du trafic de signalisation d'appel H.225.0.

Bon nombre de profils de sécurité H.235 reposent sur le modèle à routage par portier H.323, mais la Rec. UIT-T H.235.4 est davantage axée sur la sécurité des communications entre homologues, l'objectif étant de libérer les portiers des tâches de signalisation H.323 pour le routage et d'améliorer de façon générale la modulabilité et la performance. Dans la Rec. UIT-T H.235.4, qui prend en charge les appels à routage direct, les portiers opèrent surtout localement à l'intérieur de leur domaine pour réaliser l'authentification d'utilisateur/de terminal et pour assurer l'enregistrement, l'admission, la résolution d'adresse et le contrôle de largeur de bande. Quant aux terminaux, ils procèdent à l'établissement d'appel H.323 directement entre les points d'extrémité de bout en bout, comme illustré dans le scénario de la Figure 6-5.

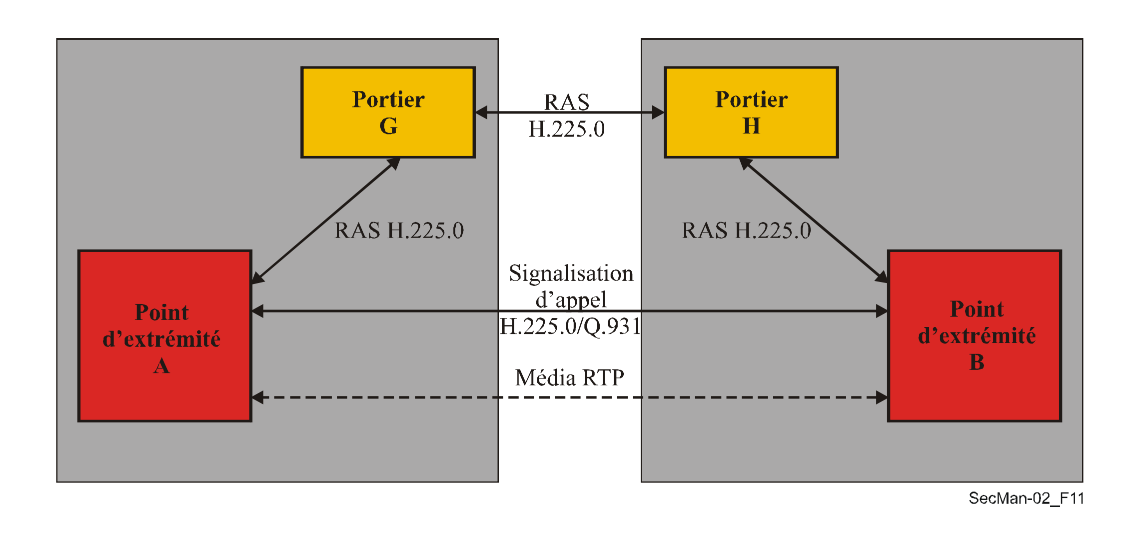


Figure 6-5 – Scénario de routage direct H.235.4

Lorsque le point d'extrémité A demande au portier G une admission d'appel pour appeler le point d'extrémité B, un portier (le portier G dans des environnements d'entreprise ou le portier H dans des environnements interdomaines) produit la clé de signalisation d'appel de bout en bout pour les deux points d'extrémité (A et B). D'une manière très proche du système Kerberos (une application figure dans la Rec. UIT-T J.191), le point d'extrémité A obtient de façon sécurisée un jeton de sécurité contenant la clé produite et obtient aussi un autre jeton de sécurité contenant la même clé pour le point d'extrémité B. Lorsqu'il lance l'appel, le point d'extrémité A applique directement la clé pour protéger la signalisation d'appel en direction du point d'extrémité B et transmet l'autre jeton de sécurité contenant la clé en direction du point d'extrémité B. Dans le cadre de la Rec. UIT-T H.235.4, il est possible d'utiliser le profil de sécurité H.235.1 ou H.235.3.

Les autres procédures relatives aux scénarios interdomaines dans la Rec. UIT-T H.235.4 permettent de distinguer les cas où les points d'extrémité ou les portiers ne prennent pas en charge la capacité de concordance de clés de Diffie-Hellman; toutefois, le résultat final est que les points d'extrémité A et B obtiennent un secret de session partagé qui protège de bout en bout la signalisation H.323 en termes d'authentification, d'intégrité ou de confidentialité.

Afin d'assurer une plus grande sécurité aux systèmes qui utilisent des numéros d'identification personnels (PIN, *personal identification number*) ou des mots de passe pour authentifier les utilisateurs, la Rec. UIT-T H.235.5 définit un "*cadre de l'authentification sécurisée pendant l'échange de messages RAS au moyen de secrets partagés faibles*" fondé sur l'utilisation de méthodes à clé

publique pour sécuriser l'utilisation des numéros PIN/mots de passe. Un profil particulier est actuellement défini, qui exploite la méthode d'échange de clés chiffrées pour négocier un secret partagé fort, protégé contre les attaques passives ou actives (attaques de l'intercepteur). Le cadre permet de définir de nouveaux profils au moyen d'autres méthodes de négociation fondées sur des clés publiques.

La Rec. UIT-T H.235.6, intitulée "*Profil pour le chiffrement vocal avec gestion de clés native dans les systèmes H.235/H.245*", rassemble toutes les procédures qui sont nécessaires pour le chiffrement du flux de médias RTP, y compris la gestion de clés associée qui est entièrement exprimée dans les champs de signalisation H.245.

Dans le souci d'assurer une meilleure convergence avec les protocoles SIP et SRTP, la Rec. UIT-T H.235.7, intitulée "*Utilisation du protocole de gestion de clés MIKEY avec le protocole de transport en temps réel sécurisé (SRTP) dans les systèmes H.235*", utilise le protocole en temps réel sécurisé (SRTP, RFC 3711) dans les systèmes H.235. Cette Recommandation spécifie comment utiliser la gestion de clés MIKEY IETF pour la distribution de clés de média SRTP de bout en bout.

Une autre approche, complémentaire, fait l'objet de la Rec. UIT-T H.235.8, intitulée "*Echange de clés dans le protocole SRTP au moyen de canaux de signalisation sécurisés*", le but étant de signaler en clair les paramètres de clé SRTP de bout en bout dans l'hypothèse d'un transport sous-jacent sécurisé, de manière analogue à l'approche considérée dans les descriptions du protocole SDP faites par l'IETF. Pour obtenir des canaux de transport de signalisation sécurisés, on peut mettre en œuvre le protocole de sécurité Internet, le protocole de sécurité de la couche de transport ou la syntaxe de message cryptographique (CMS, *cryptographic message syntax*).

La traversée de traducteurs d'adresse de réseau et de pare-feu (FW, *firewall*) par des flux de signalisation H.323 a longtemps été impossible à mettre en place dans la pratique. La Rec. UIT-T H.235.9, intitulée "*Prise en charge des passerelles de sécurité dans les systèmes H.323*", définit des procédures de sécurité qui permettent à un terminal/point d'extrémité H.323 de découvrir les passerelles de sécurité H.323, ce type d'entité étant censé comporter la fonctionnalité d'une passerelle de couche application (ALG, *application layer gateway*) NAT/FW H.323. La passerelle de signalisation H.323 de confiance considérée détecte les transactions de signalisation en cours et participe alors à la gestion de clés pour la signalisation H.225.0.

La Rec. UIT-T H.235.0 s'applique essentiellement à des environnements H.323 "statiques" avec uniquement des dispositions concernant une mobilité restreinte, mais une mobilité sécurisée des utilisateurs et des terminaux dans des environnements H.323 répartis est également nécessaire au-delà de l'interconnexion interdomaines et de la mobilité restreinte dans la zone du portier. La Rec. UIT-T H.530 répond à ces besoins de sécurité en abordant notamment les aspects de sécurité suivants:

- Authentification et autorisation d'utilisateur/de terminal mobile dans des domaines visités à l'étranger.
- Authentification du domaine visité.
- Gestion de clés sécurisée.
- Protection des données de signalisation entre un terminal mobile et un domaine visité.

La Figure 6-6 illustre le scénario de base H.530, dans lequel un terminal mobile (MT, *mobile terminal*) H.323 peut être rattaché directement à son domaine de rattachement via le portier du domaine de rattachement (H-GK, *home gatekeeper*) ou peut être rattaché à un portier d'un domaine visité (V-GK, *visited gatekeeper*). Comme le terminal mobile et l'utilisateur ne sont pas connus du domaine visité, le portier du domaine visité doit d'abord interroger la fonction d'authentification (AuF, *authentication function*) du domaine de rattachement dans lequel le terminal mobile est abonné et connu. Par conséquent, le domaine visité délègue la tâche d'authentification à la fonction AuF du domaine de rattachement et laisse à cette fonction AuF le soin de réaliser l'authentification et de décider de l'autorisation. En outre, la fonction AuF garantit au portier V-GK un lien cryptographique de la clé dynamique partagée par le terminal mobile et le portier V-GK en utilisant un protocole de sécurité cryptographique imbriqué dans les procédures H.530. La fonction AuF communique sa décision de façon sécurisée au portier du domaine visité pendant la phase d'enregistrement du terminal.

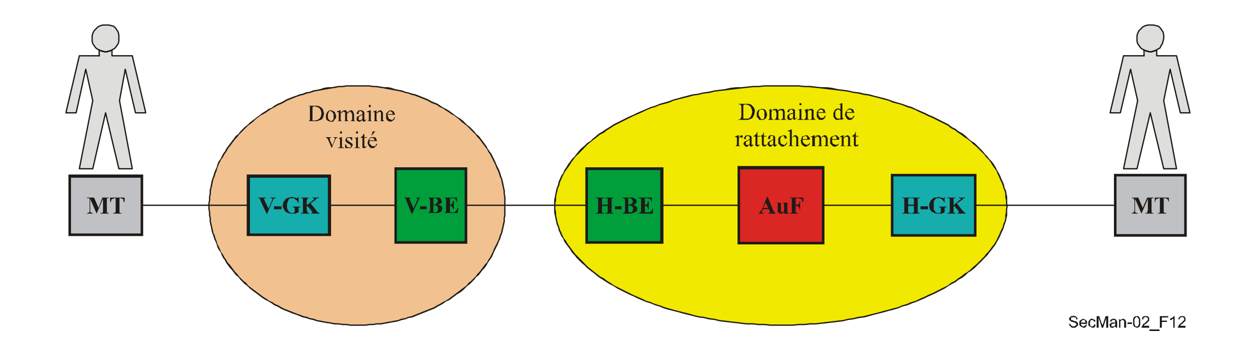


Figure 6-6 – Scénario H.530

Les communications entre le domaine visité et le domaine de rattachement utilisent le protocole générique H.501 pour la gestion de la mobilité et les communications intra et interdomaines dans les systèmes H.323. Après réception de la décision d'authentification et d'autorisation de la fonction AuF, le portier du domaine visité et le terminal mobile s'entendent sur une nouvelle clé de liaison dynamique qu'ils partagent pendant leur association de sécurité. Cette clé de liaison est utilisée pour protéger toute communication de signalisation H.323 ultérieure entre le terminal mobile et le portier V-GK; la communication de signalisation multimédia reste à l'intérieur du domaine visité et ne nécessite pas d'interaction avec le domaine de rattachement.

La Rec. UIT-T H.530 repose sur une architecture de sécurité très simple, dans laquelle le terminal mobile partage uniquement un secret partagé préconfiguré (par exemple un mot de passe d'abonnement) avec sa fonction AuF dans le domaine de rattachement mais n'a pas besoin de partager d'association de sécurité a priori avec quelque domaine visité que ce soit. La protection de sécurité entre les entités à l'intérieur d'un domaine ainsi que d'un domaine à l'autre nécessite uniquement des secrets partagés symétriques, qui peuvent par exemple être établis par le biais d'accords de niveau de service interdomaines. La Rec. UIT-T H.530 réutilise les profils de sécurité H.235 existants, par exemple le profil H.235.1 pour sécuriser les messages de signalisation H.501/H.530 d'un domaine à l'autre.

En plus de la Rec. UIT-T H.235.0, les Recommandations UIT-T H.350 et H.350.2 prévoient une gestion de clés modulable fondée sur le protocole rapide d'accès à l'annuaire (LDAP, *lightweight directory access protocol*) et la couche de connecteurs sécurisés (SSL/TLS, *secure socket layer*). La Rec. UIT-T H.350.x définit plusieurs capacités importantes qui permettent aux entreprises et aux opérateurs de procéder à une gestion sécurisée de très nombreux utilisateurs de services de vidéo et téléphonie IP. La Rec. UIT-T H.350 permet de relier les protocoles H.323, SIP, H.320 et les services de messagerie génériques à un service d'annuaire, de manière à ce que les pratiques modernes de gestion d'identité puissent être appliquées aux communications multimédias. Par ailleurs, un endroit normalisé est réservé dans l'architecture pour stocker les pouvoirs de sécurité pour ces protocoles.

La Rec. UIT-T H.350 ne modifie les architectures de sécurité d'aucun protocole. Toutefois, elle n'offre pas d'endroit normalisé pour stocker les pouvoirs d'authentification, si besoin est. Il est à noter que les protocoles H.323 et SIP prennent tous deux en charge l'authentification par secret (H.235.1 et HTTP Digest, respectivement). Ces approches nécessitent que le serveur d'appels ait accès au mot de passe. Ainsi, si un serveur d'appels ou un annuaire H.350 est compromis, des mots de passe peuvent aussi être compromis. Ces faiblesses peuvent être dues à des faiblesses des systèmes (annuaire H.350 ou serveur d'appels) et de leur fonctionnement plutôt qu'à des faiblesses du protocole H.350 proprement dit.

Il est vivement conseillé qu'un serveur d'appels et un annuaire H.350 s'authentifient mutuellement avant de partager des informations. Il est également vivement conseillé que les communications entre annuaires H.350 et serveurs d'appels ou points d'extrémité soient établies sur des voies de communication sécurisées (par exemple SSL ou TLS).

Il est à noter que les listes de contrôle d'accès dans les serveurs LDAP dépendent de la politique appliquée et ne font pas partie de la norme. Les administrateurs de système sont invités à faire preuve de bon sens lorsqu'ils établissent un contrôle d'accès sur les attributs H.350. Par exemple, les attributs de mot de passe ne devraient être accessibles que par l'utilisateur authentifié, tandis que les attributs d'adresse peuvent être rendus publics.

6.1.3 Dispositifs H.323 et NAT/FW

L'Internet a été conçu suivant le principe "de bout en bout". Autrement dit, deux dispositifs quelconques raccordés au réseau peuvent communiquer directement entre eux. Toutefois, en raison de préoccupations liées à la sécurité et d'un manque d'adresses de réseau IPv4, des pare-feu et des traducteurs d'adresse de réseau sont souvent employés à la frontière des réseaux. Ces frontières concernent le domaine de la résidence, le domaine du fournisseur de services, le domaine de l'entreprise et quelquefois le domaine du pays. Parfois, plusieurs pare-feu ou dispositifs NAT sont employés dans un même domaine.

Les pare-feu sont conçus pour contrôler de façon stricte le passage des informations à travers les frontières de réseau et sont généralement configurés pour bloquer la plupart des communications IP. Si un pare-feu n'est pas configuré explicitement pour laisser passer le trafic H.323 provenant de dispositifs externes afin que ce trafic aboutisse aux dispositifs H.323 internes, la communication est tout simplement impossible, ce qui pose problème pour tout utilisateur d'équipement H.323.

Les traducteurs NAT traduisent les adresses utilisées dans le domaine interne en adresses utilisées dans le domaine externe et inversement. Les adresses utilisées dans un domaine résidentiel ou dans un domaine d'entreprise sont généralement, mais pas toujours, attribuées à partir des espaces d'adresses de réseau privé définis dans la norme RFC 1597, qui sont les suivants:

Classe	Intervalle d'adresses	Nombre d'adresses IP
A	10.0.0.0 – 10.255.255.255	16,777,215
B	172.16.0.0 – 172.31.255.255	1,048,575
C	192.168.0.0 – 192.168.255.255	65,535

Les dispositifs NAT posent un problème encore plus frustrant à la plupart des protocoles IP, en particulier ceux qui acheminent des adresses IP dans le protocole. Les protocoles H.323, SIP et d'autres protocoles de communication en temps réel qui fonctionnent sur des réseaux à commutation par paquets doivent fournir des informations de port et d'adresse IP de sorte que les autres participants à la communication sachent où envoyer les flux de média (par exemple flux audio et vidéo).

L'UIT-T a étudié les problèmes posés par la traversée des dispositifs NAT/FW et a élaboré une série de trois Recommandations pour permettre aux flux provenant de systèmes H.323 de traverser de façon transparente un ou plusieurs dispositifs NAT/FW. Il s'agit des Recommandations UIT-T H.460.17 ("*Utilisation de la connexion de signalisation d'appel H.225.0 pour le transport de messages RAS H.323*"), H.460.18 ("*Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de signalisation H.323*") et H.460.19 ("*Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de média H.323*").

Toutes ces Recommandations utilisent le cadre d'extensibilité générique présenté dans la version 4 de la Rec. UIT-T H.323, ce qui signifie que tout dispositif H.323 de version 4 ou d'une version supérieure peut être adapté pour prendre en charge ces procédures de traversée de dispositifs NAT/FW. Par ailleurs, des dispositions ont été définies dans la Rec. UIT-T H.460.18 pour permettre aux flux provenant d'anciens dispositifs non compatibles avec ces Recommandations de traverser correctement les dispositifs NAT/FW avec l'aide d'un "proxy".

La Figure 6-7 montre comment un "proxy" spécial pourrait être utilisé pour permettre aux flux provenant de dispositifs "non compatibles" NAT/FW de traverser facilement et correctement les dispositifs NAT/FW:

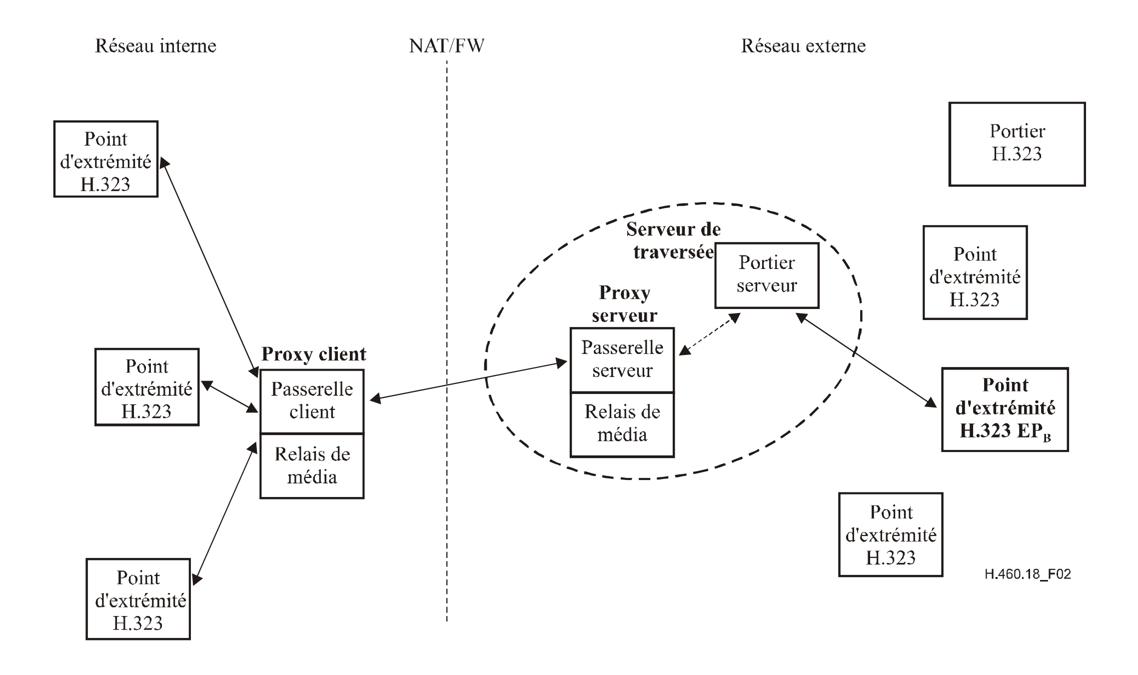


Figure 6-7 – Architecture H.460.18 avec décomposition totale

La topologie ci-dessus peut aussi être souhaitable dans les cas où, par exemple, une entreprise souhaite contrôler la route que les flux de signalisation d'appel et de média H.323 empruntent dans le réseau. Toutefois, les Recommandations UIT-T H.460.17 et H.460.18 (qui portent sur les aspects de signalisation relatifs à la traversée de dispositifs NAT/FW) permettent aux flux provenant de points d'extrémité de traverser les dispositifs NAT/FW sans l'aide d'un "proxy" interne spécial. La Figure 6-8 illustre la topologie correspondante:

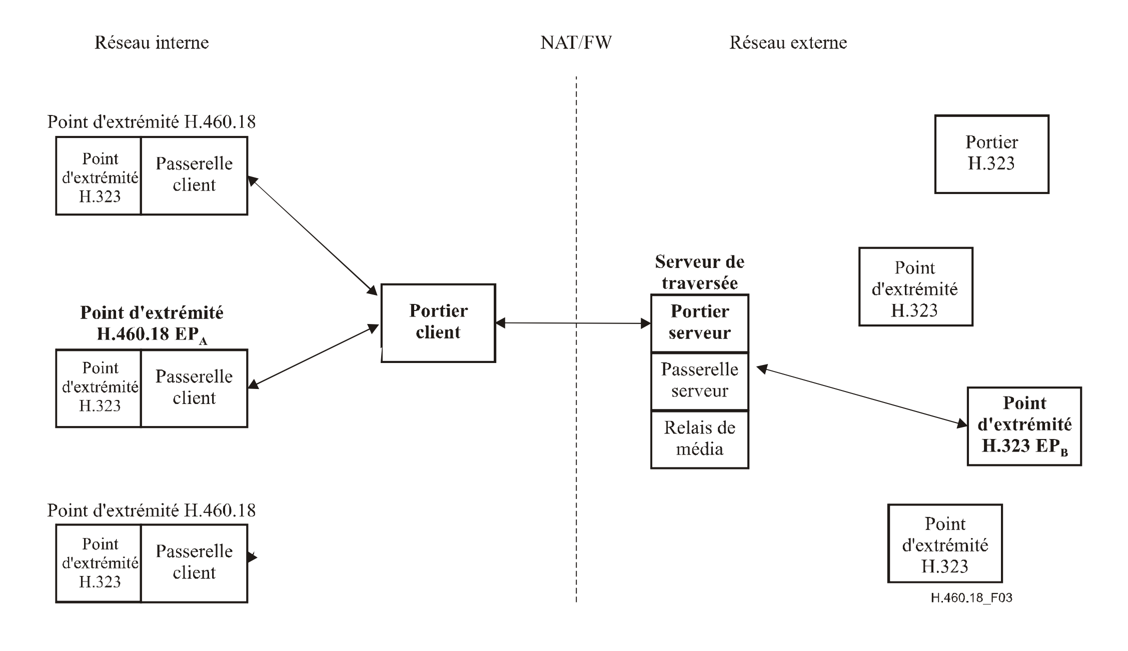


Figure 6-8 – Architecture avec communication entre portiers

Dans la topologie H.460.18 ci-dessus, les points d'extrémité raccordés au réseau interne communiquent avec le portier qui réside également dans le réseau interne pour résoudre l'adresse des entités externes (par exemple une adresse IP obtenue à partir d'un numéro de téléphone ou d'une adresse URL H.323). Le portier situé dans le réseau interne communique avec un portier situé dans le réseau externe pour échanger ces informations d'adressage et achemine ces informations au point d'extrémité appelant. Lorsqu'un dispositif situé dans le réseau interne lance un appel à destination d'un dispositif situé dans le réseau externe, il utilisera les procédures H.460.18 pour ouvrir les "microtrous" nécessaires dans les dispositifs NAT/FW pour laisser passer la signalisation du réseau interne au réseau externe. Il utilisera en outre les procédures H.460.19 pour ouvrir les "microtrous" nécessaires pour permettre aux flux de médias de passer correctement du réseau interne au réseau externe et inversement.

Lorsque les dispositifs appelant et appelé résident dans des réseaux privés différents séparés par des dispositifs NAT/FW et l'Internet public, au moins une "passerelle serveur" et un "relais de média" (définis dans la Rec. UIT-T H.460.18) sont nécessaires pour pouvoir acheminer correctement la signalisation et les médias entre les deux réseaux privés. Cette combinaison de dispositifs est généralement appelée "contrôleur de limite de session". La raison en est simple: par conception, un paquet IP provenant d'un réseau privé ne peut pénétrer dans un autre réseau privé qu'avec l'aide d'une entité ("proxy") du réseau public.

Bien entendu, les appels qui proviennent et aboutissent dans un même réseau privé continuent à se dérouler comme avant, sans procédures spéciales de traitement d'appel; les Recommandations UIT-T H.460.17, H.460.18 et H.460.19 n'ont aucune incidence sur le fonctionnement des dispositifs H.323 qui se trouvent dans le même réseau interne.

6.2 Système IPCablecom

Le système IPCablecom permet aux opérateurs de télévision par câble d'offrir des services basés sur IP en temps réel (par exemple des communications téléphoniques) sur leurs réseaux qui ont été améliorés pour prendre en charge des câblo-modems. L'architecture du système IPCablecom est définie dans la Rec. UIT-T J.160. A un très haut niveau, l'architecture IPCablecom repose sur trois réseaux: le "réseau d'accès HFC J.112", le "réseau IP géré" et le RTPC. Le nœud d'accès (AN, *access node*) assure la connectivité entre le "réseau d'accès HFC J.112" et le "réseau IP géré". La passerelle de signalisation (SG, *signalling gateway*) et la passerelle média (MG, *media gateway*) assurent la connectivité entre le "réseau IP géré" et le RTPC. La Figure 6-9 illustre l'architecture IPCablecom de référence.

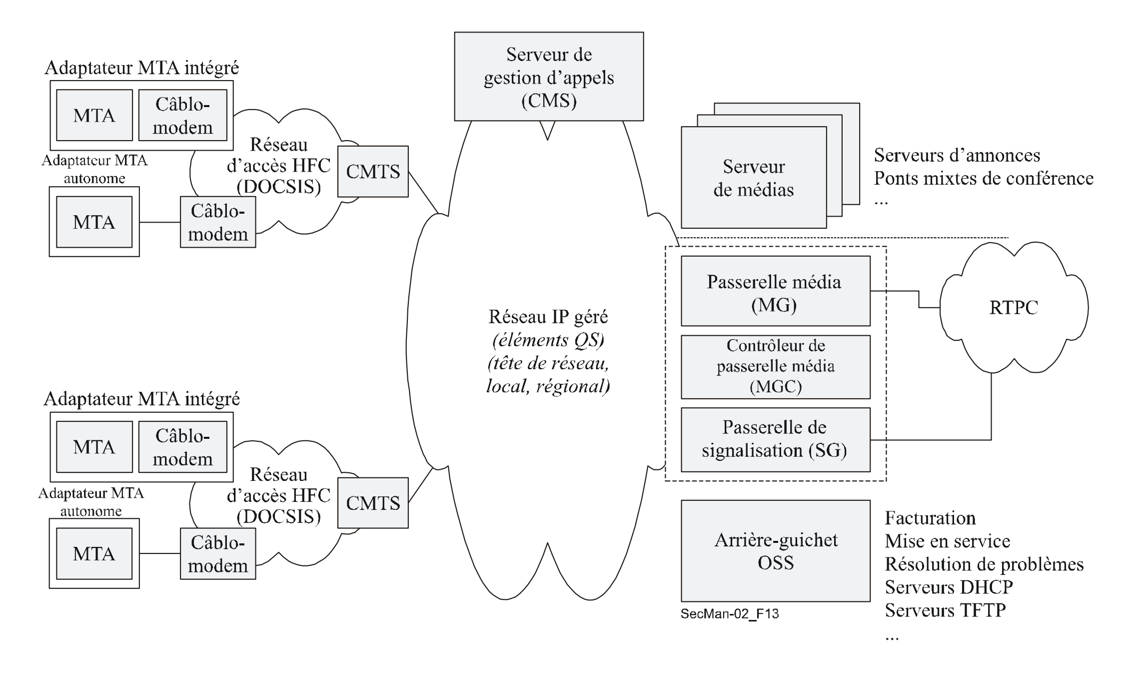


Figure 6-9 – Architecture IPCablecom de référence [J.165]

Le réseau d'accès hybride fibre optique/câble coaxial (HFC, *hybrid fibre-coaxial cable*) J.112 assure un transport à haut débit, fiable et sécurisé entre les locaux de l'abonné et la tête de réseau câblé. Ce réseau d'accès peut offrir toutes les capacités J.112 (dont la qualité de service) et des interfaces avec la couche physique par le biais d'un système de terminaison de câblo-modem (CMTS, *cable modem termination system*).

Le réseau IP géré fournit plusieurs fonctions. Il offre tout d'abord l'interconnexion entre les composants fonctionnels IPCablecom fondamentaux chargés de la signalisation, de la transmission de média, de la mise en service et de l'établissement de la qualité de service. Par ailleurs, il assure la connectivité IP longue distance entre les autres réseaux IP gérés et les réseaux HFC J.112. Le réseau IP géré est constitué des composants fonctionnels suivants: serveur de gestion d'appels, serveur d'annonces, passerelle de signalisation, passerelle média, contrôleur de passerelle média et plusieurs serveurs d'arrière du système d'assistance à l'exploitation (OSS, *operational support system*).

Le *serveur de gestion d'appels* (CMS, *call management server*) offre des services liés à la commande et à la signalisation d'appel à l'adaptateur de terminal média (MTA, *media terminal adapter*), au nœud d'accès et aux passerelles RTPC du réseau IPCablecom. Le serveur CMS est un élément de réseau sécurisé qui se trouve dans la partie IP gérée du réseau IPCablecom. Les *serveurs d'annonces* sont des composants de réseau logiques qui gèrent et passent des tonalités et messages d'information en réponse à des événements qui se produisent dans le réseau. La fonction de *passerelle de signalisation* envoie et reçoit la signalisation de réseau à commutation de circuit à la frontière du réseau IPCablecom. Pour le système IPCablecom, cette fonction ne prend en charge que la signalisation autre que service par service sous la forme de messages SS7 (la signalisation service par service sous la forme de tonalités multifréquences est directement prise en charge par la fonction de passerelle média). Le *contrôleur de passerelle média* (MGC, *media gateway controller*) sert d'intermédiaire entre le réseau IPCablecom et le RTPC concernant les informations de signalisation d'appel. Il maintient et contrôle l'état d'appel global pour les appels nécessitant une interconnexion avec le RTPC. La *passerelle média* (MG, *media gateway*) assure la connectivité des supports entre le RTPC et le réseau IPCablecom. Chaque support est représenté sous la forme d'un point d'extrémité et le contrôleur MGC charge la passerelle média d'établir et de contrôler les connexions de média vers les autres points d'extrémité du réseau IPCablecom. Le contrôleur MGC charge également la passerelle média de détecter et de générer des événements et des signaux relatifs à l'état d'appel. Le *système arrière-guichet OSS* contient des composants de gestion commerciale, de gestion de service et de gestion de réseau servant d'appui aux processus d'exploitation centraux. Les principales fonctions du système OSS sont les suivantes: gestion des défauts, gestion de la qualité de fonctionnement, gestion de la sécurité, gestion de la comptabilité et gestion de la configuration. L'architecture IPCablecom définit un ensemble limité de composants fonctionnels et d'interfaces OSS pour prendre en charge la configuration des dispositifs MTA et la messagerie d'événements en vue de l'acheminement des informations de facturation.

6.2.1 Problèmes de sécurité dans le système IPCablecom

Chacune des interfaces de protocole IPCablecom est exposée à des menaces qui peuvent entraîner des risques de sécurité à la fois pour l'abonné et pour le fournisseur de services. Par exemple, le trajet du flux de média peut emprunter un grand nombre de connexions d'opérateurs de réseaux dorsaux qui peuvent être inconnus. Le flux de média est alors vulnérable aux écoutes malveillantes entraînant une perte de la confidentialité des communications.

6.2.2 Mécanismes de sécurité dans le système IPCablecom

Dans le système IPCablecom, la sécurité est implémentée dans les éléments les plus bas de la pile et utilise donc essentiellement des mécanismes définis par l'IETF. L'architecture IPCablecom fait face aux menaces en spécifiant, pour chaque interface de protocole définie, les mécanismes de sécurité sous-jacents (tels que IPsec) qui offrent à l'interface les services de sécurité dont elle a besoin. Dans le contexte de l'architecture X.805, les services de sécurité définis pour IPCablecom concernent les neuf cellules résultant des trois plans et des trois couches de la Figure 2-1. Par exemple, les services de

sécurité des protocoles de signalisation pour le plan de commande sont assurés par le protocole IPSec. La sécurité de l'infrastructure de gestion est obtenue grâce au protocole SNMPv3.

Les services de sécurité disponibles par l'intermédiaire de la couche des services essentiels de l'architecture IPCablecom sont les suivants: authentification, contrôle d'accès, intégrité, confidentialité et non-répudiation. Une interface de protocole IPCablecom peut employer zéro, un ou plusieurs de ces services pour répondre à ses besoins de sécurité particuliers.

La sécurité IPCablecom répond aux exigences de sécurité de chaque interface de protocole constituante en:

- identifiant le modèle de menaces propre à chaque interface de protocole constituante;
- identifiant les services de sécurité (authentification, autorisation, confidentialité, intégrité et non-répudiation) requis pour faire face aux menaces identifiées;
- spécifiant le mécanisme de sécurité particulier qui assure les services de sécurité requis.

Les mécanismes de sécurité comprennent à la fois le protocole de sécurité (par exemple IPsec, sécurité de couche RTP et sécurité SNMPv3) et le protocole de gestion de clés support (par exemple IKE, PKINIT/Kerberos). Par ailleurs, les services essentiels de sécurité IPCablecom incluent un mécanisme assurant le chiffrement de bout en bout des flux de média RTP, ce qui réduit fortement la menace de perte de confidentialité. La Figure 6-10 récapitule toutes les interfaces de sécurité IPCablecom. Si le protocole de gestion de clés n'est pas indiqué, c'est qu'il n'est pas nécessaire pour l'interface considérée. Les interfaces IPCablecom qui n'ont pas besoin de sécurité ne sont pas représentées sur la Figure 6-10.

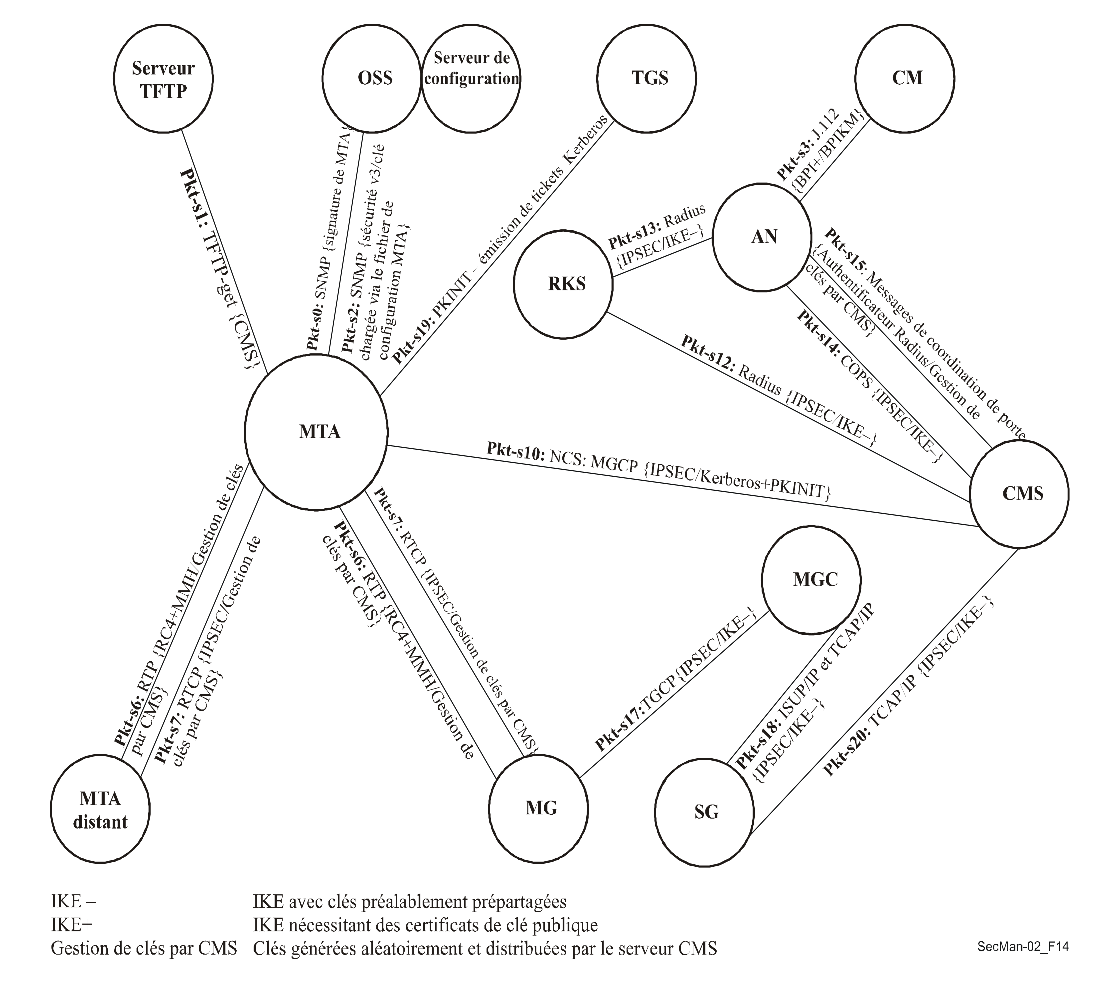


Figure 6-10 – Interfaces de sécurité IPCablecom (étiquetées sous la forme <étiquette>: <protocole> { <protocole de sécurité> / <protocole de gestion de clés > })

L'architecture de sécurité IPCablecom subdivise la mise en service de dispositif en trois activités distinctes: inscription de l'abonné, mise en service du dispositif et autorisation du dispositif. Le processus d'*inscription de l'abonné* établit un compte permanent de facturation de l'abonné qui identifie de manière univoque l'adaptateur MTA auprès du serveur CMS grâce au numéro de série ou à l'adresse MAC de l'adaptateur MTA. Le compte de facturation sert également à identifier les services auxquels l'abonné a souscrit pour l'adaptateur MTA. L'inscription de l'abonné peut se faire dans la bande ou hors bande. La spécification proprement dite du processus d'inscription de l'abonné sort du cadre de l'architecture IPCablecom et peut varier d'un fournisseur de service à l'autre. Pour la *mise en service du dispositif*, l'adaptateur MTA vérifie l'authenticité du fichier de configuration qu'il télécharge en commençant par établir la sécurité SNMPv3 (en utilisant une authentification de type Kerberos et une gestion de clés) entre lui-même et le serveur de mise en service. Le serveur de mise en service fournit ensuite à l'adaptateur MTA l'emplacement du fichier de configuration et une valeur de hachage du fichier de configuration. L'adaptateur MTA extrait le fichier de configuration, applique un hachage au fichier de configuration et compare le résultat avec la valeur de hachage que le serveur de mise en service lui a fournie. Le fichier de configuration est authentifié si les valeurs de hachage concordent. Le fichier de configuration peut facultativement être chiffré à des fins de confidentialité (la confidentialité SNMPv3 doit aussi être prise en charge afin d'assurer une transmission sécurisée de la clé de chiffrement du fichier de configuration à l'adaptateur MTA). L'*autorisation du dispositif* est le processus selon lequel l'adaptateur MTA mis en service s'authentifie auprès du serveur de gestion d'appels et établit une association de sécurité avec ce serveur avant de devenir entièrement opérationnel. L'autorisation de dispositif permet de protéger la signalisation d'appel subséquente dans le cadre de l'association de sécurité établie.

Il est possible de protéger à la fois le trafic de signalisation et les flux de média. L'ensemble du trafic de signalisation, qui comprend la signalisation de qualité de service, la signalisation d'appel et la signalisation avec l'interface de passerelle RTPC, sera sécurisé au moyen du protocole IPsec. Les associations de sécurité IPsec seront gérées grâce à l'utilisation de deux protocoles de gestion de clés: Kerberos/PKINIT et IKE. Le protocole Kerberos/PKINIT sera utilisé pour échanger des clés entre des clients d'adaptateur MTA et leur serveur CMS; le protocole IKE sera utilisé pour gérer toutes les autres associations de sécurité IPsec de signalisation. En ce qui concerne les flux de média, chaque paquet RTP de média est chiffré aux fins de confidentialité et authentifié afin de vérifier l'intégrité et l'origine du paquet. Les adaptateurs MTA ont la capacité de négocier un algorithme de chiffrement particulier, bien que le seul algorithme de chiffrement requis soit AES. Chaque paquet RTP peut facultativement inclure un code d'authentification de message (MAC, *message authentication code*). L'algorithme de calcul du code MAC peut aussi être négocié, bien que le seul à être actuellement spécifié soit MMH. Le calcul du code MAC englobe l'en-tête non chiffré et la charge utile chiffrée du paquet.

Les clés de chiffrement et le calcul du code MAC sont déterminés à partir du secret de bout en bout et des données de remplissage facultatives, qui sont échangés entre les adaptateurs MTA d'émission et de réception dans le cadre de la signalisation d'appel. Les échanges de clés pour la sécurité des flux de média sont donc eux-mêmes sécurisés par la protection de la signalisation d'appel.

La sécurité est également assurée pour le système OSS et le système de facturation. Les agents SNMP présents dans les dispositifs IPCablecom implémentent le protocole SNMPv3. Le modèle de sécurité d'utilisateur SNMPv3 [RFC 2274] offre des services d'authentification et de confidentialité concernant le trafic SNMP. Le contrôle d'accès de type vue SNMPv3 [RFC 2275] peut être utilisé pour le contrôle d'accès à des objets MIB.

Le protocole de gestion de clés IKE sert à établir des clés de chiffrement et d'authentification entre le serveur d'archivage (RKS, *record keeping server*) et chaque élément de réseau IPCablecom qui génère des messages d'événement. Lorsque des associations de sécurité IPsec de réseau sont établies, ces clés doivent être créées entre chaque serveur RKS (primaire, secondaire, etc.) et chaque serveur CMS et nœud d'accès. Un échange de clés entre le contrôleur MGC et le serveur RKS peut être prévu; il appartient aux fabricants de l'implémenter ou non dans la phase 1 de l'architecture IPCablecom. Les messages d'événement sont envoyés par le serveur CMS et par le nœud d'accès au serveur RKS au moyen du protocole de transport RADIUS, qui est lui-même sécurisé par IPsec.

6.3 Transmission de télécopie sécurisée

La télécopie est une application très courante. La transmission de télécopie était définie au départ sur le RTPC (Rec. UIT-T T.4), puis également sur le RNIS (Rec. UIT-T T.6) et, plus récemment, aussi sur les réseaux IP (y compris l'Internet) pas en temps réel – relais par messagerie électronique – (Rec. UIT-T T.37) ou en temps réel – en utilisant le protocole RTP – (Rec. UIT-T T.38). Deux problèmes de sécurité généralement rencontrés par la transmission de télécopie – que le réseau soit un RTPC, un RNIS ou un réseau IP – concernent l'authentification (et parfois la non-répudiation) d'une connexion et la confidentialité des données transmises. Ces problèmes sont d'autant plus importants pour les protocoles T.37 et T.38 que le réseau IP est, par nature, réparti.

La Rec. UIT-T T.36 définit deux solutions techniques indépendantes qui peuvent être utilisées dans le contexte de la transmission de télécopie sécurisée pour le chiffrement des documents échangés. Les deux solutions techniques s'appuient sur les algorithmes HKM/HFX40 (Annexe A/T.36) et l'algorithme RSA (Annexe B/T.36). Même si les deux limitent les clés de session à 40 bits (en raison de réglementations nationales au moment de l'approbation de la Recommandation, 1997), un mécanisme est spécifié afin de générer une clé de session redondante (à partir d'une clé de session de 40 bits) pour les algorithmes qui nécessitent des clés plus longues. L'Annexe C/T.36 décrit l'utilisation du système HKM offrant des capacités de gestion de clés sécurisée pour les télécopieurs grâce à un enregistrement unidirectionnel entre les entités X et Y ou à la transmission sécurisée d'une clé secrète entre les entités X et Y. L'Annexe D/T.36 définit les procédures d'utilisation du système de chiffrement HFX40 qui permet d'assurer la confidentialité des messages de télécopie. Enfin, l'Annexe E/T.36 décrit l'utilisation de l'algorithme de hachage HFX40-I, les calculs nécessaires et les informations à échanger entre les télécopieurs afin d'assurer l'intégrité d'un message de télécopie transmis, cet algorithme étant choisi ou préprogrammé en remplacement du chiffrement du message.

De plus, la Rec. UIT-T T.36 définit les services de sécurité suivants:

- Authentification mutuelle (obligatoire).
- Service de sécurité (facultatif) incluant l'authentification mutuelle, l'intégrité de message et la confirmation de réception de message.
- Service de sécurité (facultatif) incluant l'authentification mutuelle, la confidentialité de message (chiffrement) et l'établissement de clé de session.
- Service de sécurité (facultatif) incluant l'authentification mutuelle, l'intégrité de message, la confirmation de réception de message, la confidentialité de message (chiffrement) et l'établissement de clé de session.

Quatre profils de service sont définis sur la base des services de sécurité énumérés ci-dessus, comme indiqué dans le Tableau 6-1 ci-dessous.

Tableau 6-1 – Profils de sécurité de l'Annexe H/T.30

Services de sécurité	Profils de service			
	1	2	3	4
Authentification mutuelle	X	X	X	X
• Intégrité de message • Confirmation de réception de message		X		X
• Confidentialité de message (chiffrement) • Etablissement de clé de session			X	X

6.3.1 Sécurité de la transmission de télécopie fondée sur les systèmes HKM et HFX

La combinaison des systèmes HKM (*hawthorne key management*) et HFX (*Hawthorne Facsimile Cipher*) offre les capacités de sécurité suivantes concernant les communications de document entre entités (terminaux ou opérateurs de terminal):

- authentification mutuelle d'entités;
- établissement de clé de session secrète;
- confidentialité de document;
- confirmation de réception;
- confirmation ou réfutation d'intégrité de document.

La gestion de clés est assurée par le système HKM défini dans l'Annexe B/T.36. Deux procédures sont définies, la première étant l'enregistrement et la seconde la transmission sécurisée d'une clé secrète. L'enregistrement établit des secrets mutuels et permet de sécuriser toutes les transmissions suivantes. Dans les transmissions suivantes, le système HKM assure l'authentification mutuelle, établit une clé de session secrète pour la confidentialité et l'intégrité de document et prend en charge la confirmation de réception et la confirmation ou la réfutation d'intégrité de document.

La confidentialité de document est assurée par le système de chiffrement défini dans l'Annexe D/T.36. Ce système utilise une clé de 12 chiffres décimaux, ce qui correspond approximativement à une clé de session de 40 bits.

L'intégrité de document est assurée par le système défini dans l'Annexe E/T.36 et la Rec. UIT-T T.36 définit l'algorithme de hachage, y compris les calculs et l'échange d'informations associés.

Dans le mode enregistrement, les deux terminaux échangent des informations qui permettent aux entités de s'identifier mutuellement de manière univoque. Dans ce mode, les utilisateurs conviennent d'une clé secrète à usage unique. Chaque entité stocke un nombre de 16 chiffres qui est associé de manière univoque à l'entité avec laquelle elle a procédé à l'enregistrement.

Lorsqu'un terminal émetteur doit procéder à l'envoi sécurisé d'un document, il envoie à l'entité réceptrice le nombre secret de 16 chiffres associé à l'entité réceptrice ainsi qu'un nombre aléatoire et une clé de session chiffrée en tant qu'épreuve. Le terminal récepteur répond en envoyant la clé de 16 chiffres associée à l'entité émettrice ainsi qu'un nombre aléatoire et une version rechiffrée de l'épreuve provenant de l'entité émettrice. En même temps, il envoie à l'entité émettrice un nombre aléatoire et une clé de session chiffrée en tant qu'épreuve. Le terminal émetteur répond par un nombre aléatoire et une version rechiffrée de l'épreuve provenant de l'entité réceptrice. Cette procédure permet aux deux entités de s'authentifier mutuellement. En même temps, le terminal émetteur envoie un nombre aléatoire et la clé de session chiffrée à utiliser pour le chiffrement et le hachage.

Après la transmission du document, le terminal émetteur envoie à l'entité réceptrice un nombre aléatoire et une clé de session chiffrée en tant qu'épreuve. En même temps, il envoie un nombre aléatoire et une valeur de hachage chiffrée permettant à l'entité réceptrice de vérifier l'intégrité du document reçu. Le terminal récepteur envoie un nombre aléatoire et la version rechiffrée de l'épreuve provenant de l'entité émettrice. En même temps, il envoie un nombre aléatoire et un message d'intégrité chiffré pour confirmer ou réfuter l'intégrité du document reçu. L'algorithme de hachage utilisé pour l'intégrité du document est appliqué à l'ensemble du document.

Un mode de remplacement est prévu, qui ne fait pas intervenir d'échange de signaux de sécurité entre les deux terminaux. Les utilisateurs s'entendent sur une clé de session secrète à usage unique qui doit être saisie manuellement. Le terminal émetteur utilise cette clé pour chiffrer le document et le terminal récepteur l'utilise pour déchiffrer le document.

6.3.2 Sécurité de la transmission de télécopie fondée sur l'algorithme RSA

L'Annexe H/T.30 spécifie les mécanismes permettant d'offrir des éléments de sécurité sur la base du mécanisme cryptographique RSA (*Rivest, Shamir & Adleman*). Pour avoir des détails sur l'algorithme RSA, on se reportera au document [*ApplCryp, pages 466 à 474*]. N'importe lequel des systèmes de codage définis dans les Recommandations UIT-T T.4 et T.30 (Huffman modifié, MR, MMR, mode caractère tel que défini dans l'Annexe D/T.4, BFT, autre mode de transfert de fichier défini dans l'Annexe C/T.4) est applicable dans le cas d'un document transmis sous couvert d'éléments de sécurité.

L'algorithme de base utilisé pour la signature numérique (services des types authentification et intégrité) est l'algorithme RSA utilisant une paire "clé publique"/"clé secrète".

Lorsque le service facultatif de confidentialité est offert, le jeton contenant la clé de session "Ks" utilisée pour le chiffrement du document, est chiffré, lui aussi, au moyen de l'algorithme RSA. La paire de clés utilisée à cette fin, appelée "clé publique de chiffrement"/"clé secrète de chiffrement", n'est pas la même que celle qui est utilisée pour les services des types authentification et intégrité. Ainsi, les deux types d'utilisation sont découplés.

L'implémentation de l'algorithme RSA utilisé dans l'Annexe H/T.30 est décrite dans la norme ISO/CEI 9796 (*Schémas de signature numérique rétablissant le message*).

Concernant le chiffrement du jeton contenant la clé de session, les règles de redondance appliquées lors de l'utilisation de l'algorithme RSA sont les mêmes que celles qui sont spécifiées dans la norme ISO/CEI 9796. Il est à noter que certaines administrations pourront exiger l'implémentation de l'algorithme DSA (*digital signature algorithm*) [*ApplCryp, pages 483 à 502*] en plus de l'algorithme RSA.

Par défaut, les *autorités de certification* ne sont pas utilisées dans le schéma de l'Annexe H/T.30, elles peuvent toutefois être facultativement utilisées pour certifier la validité de la clé publique de l'émetteur du message de télécopie. En pareil cas, la clé publique peut être certifiée conformément aux spécifications figurant dans la Rec. UIT-T X.509. La méthode à utiliser pour transmettre le certificat de la clé publique de l'émetteur est décrite à l'Annexe H/T.30, mais le format précis du certificat sera étudié ultérieurement et la transmission effective du certificat est négociée dans le protocole.

Un *mode enregistrement* est prévu en tant que fonctionnalité obligatoire. Il permet à l'émetteur et au récepteur d'enregistrer et de stocker les clés publiques de l'autre partie de manière fiable avant toute communication de télécopie sécurisée entre les deux parties. Le mode enregistrement permet d'éviter à l'utilisateur de devoir saisir manuellement les clés publiques de ses correspondants, qui sont relativement longues (64 octets au moins).

Comme le mode enregistrement permet d'échanger les clés publiques et de les stocker dans les terminaux, il n'est pas nécessaire de les transmettre pendant les communications de télécopie.

Comme décrit dans cette annexe, certaines signatures sont appliquées au résultat d'une "fonction de hachage".

Les fonctions de hachage qui peuvent être utilisées sont l'algorithme SHA-1 (*secure hash algorithm*), élaboré par le National Institute of Standards and Technology (NIST) aux Etats-Unis d'Amérique, ou le MD-5 (RFC 1321). Dans le cas de SHA-1, la longueur du résultat du processus de hachage est de 160 bits et dans le cas de MD-5, la longueur du résultat du processus de hachage est de 128 bits. Un terminal conforme à l'Annexe H/T.30 peut implémenter soit le SHA-1, soit le MD-5 soit les deux. L'utilisation de l'un ou l'autre algorithme est négociée dans le protocole (voir plus loin).

Le chiffrement des données aux fins de confidentialité est facultatif. Cinq mécanismes de chiffrement facultatifs sont enregistrés dans le cadre de l'Annexe H/T.30: FEAL-32, SAFER K.64, RC5, IDEA et HFX40 (comme décrit dans la Rec. UIT-T T.36). Dans certains pays, leur utilisation peut être assujettie à la réglementation nationale.

Il est aussi permis d'employer d'autres algorithmes facultatifs, choisis conformément à la série de normes ISO/CEI 18033.

La capacité du terminal à manipuler l'un de ces algorithmes et l'utilisation effective d'un algorithme particulier pendant une communication donnée sont négociées dans le protocole. Une clé de session est utilisée pour le chiffrement. La longueur de base d'une clé de session est de 40 bits. Pour les algorithmes qui utilisent une clé de session de 40 bits (par exemple HFX40), la clé de session "Ks" est la clé effectivement utilisée dans l'algorithme de chiffrement et pour les algorithmes qui nécessitent des clés plus longues que 40 bits (par exemple les algorithmes FEAL-32, IDEA et SAFER K-64 qui nécessitent respectivement des clés de 64 bits, 128 bits et 64 bits), un mécanisme de redondance est exécuté afin d'obtenir la longueur nécessaire. La clé résultante est appelée "clé de session redondante". La "clé de session redondante" est la clé qui est effectivement utilisée dans l'algorithme de chiffrement.

6.4 Applications de gestion de réseau

Compte tenu de l'architecture de sécurité examinée au § 2.4, il est impératif de sécuriser le trafic dans le plan de gestion. Ce trafic est utilisé pour surveiller et contrôler le réseau de télécommunication. Le trafic de gestion est généralement classé dans différentes catégories en fonction des informations requises pour exécuter les fonctions de gestion des défauts, de la configuration, de la qualité de fonctionnement, de la comptabilité et de la sécurité. La gestion de la sécurité concerne à la fois l'établissement d'un réseau de gestion sécurisé et la gestion de la sécurité des informations liées aux trois plans de sécurité et aux trois couches de sécurité de l'architecture de sécurité. Le deuxième point est décrit dans le présent paragraphe.

Traditionnellement, dans le réseau de télécommunication, le trafic de gestion est souvent transmis dans un réseau distinct qui achemine uniquement le trafic de gestion de réseau et non le trafic des utilisateurs. Ce réseau, souvent appelé réseau de gestion des télécommunications (RGT), est décrit dans la Rec. UIT-T M.3010. Le RGT est séparé et isolé de l'infrastructure du réseau public de sorte que les perturbations dues à des menaces de sécurité dans le plan d'utilisateur final du réseau public ne s'étendent pas au RGT. Compte tenu de cette séparation, il est relativement facile de sécuriser le trafic du réseau de gestion car l'accès au plan de gestion est restreint aux administrateurs de réseau autorisés et le trafic est restreint aux activités de gestion valables. Avec la mise en place des réseaux de prochaine génération, le trafic des applications d'utilisateur final risque parfois d'être combiné au trafic de gestion. Cette approche, fondée sur une seule infrastructure de réseau intégrée, permet de minimaliser les coûts mais pose bon nombre de nouveaux problèmes de sécurité. Les menaces dans le plan d'utilisateur final constituent alors des menaces pour les plans de gestion et de commande. Le plan de gestion devient alors accessible à une multitude d'utilisateurs finaux et de nombreux types d'activités malveillantes deviennent possibles.

Pour pouvoir offrir une solution complète de bout en bout, toutes les mesures de sécurité (par exemple contrôle d'accès, authentification) doivent être appliquées à chaque type d'activité de réseau (c'est-à-dire activité du plan de gestion, activité du plan de commande et activité du plan d'utilisateur final) concernant l'infrastructure du réseau, les services de réseau et les applications de réseau. Il existe un certain nombre de Recommandations de l'UIT-T qui portent tout particulièrement sur l'aspect de sécurité du plan de gestion en ce qui concerne les éléments de réseau (NE, *network element*) et les systèmes de gestion (MS, *management system*) qui font partie de l'infrastructure du réseau.

Comme décrit ci-dessus, de nombreuses normes visent à sécuriser les informations de gestion nécessaires au maintien de l'infrastructure des télécommunications, mais un autre domaine qui relève de la gestion concerne les environnements dans lesquels différents fournisseurs de services doivent interagir pour offrir des services de bout en bout, par exemple une ligne louée entre des abonnés se trouvant de part et d'autre d'une frontière géographique ou pour des organismes de réglementation ou des organismes publics en vue d'assurer le retour à la normale après une catastrophe.

6.4.1 Architecture de gestion de réseau

L'architecture permettant de définir la gestion d'un réseau de télécommunication est définie dans la Rec. UIT-T M.3010 et l'architecture physique est représentée sur la Figure 6-11. Le réseau de gestion définit des interfaces qui déterminent les échanges requis pour assurer les fonctions OAM&P à différents niveaux.

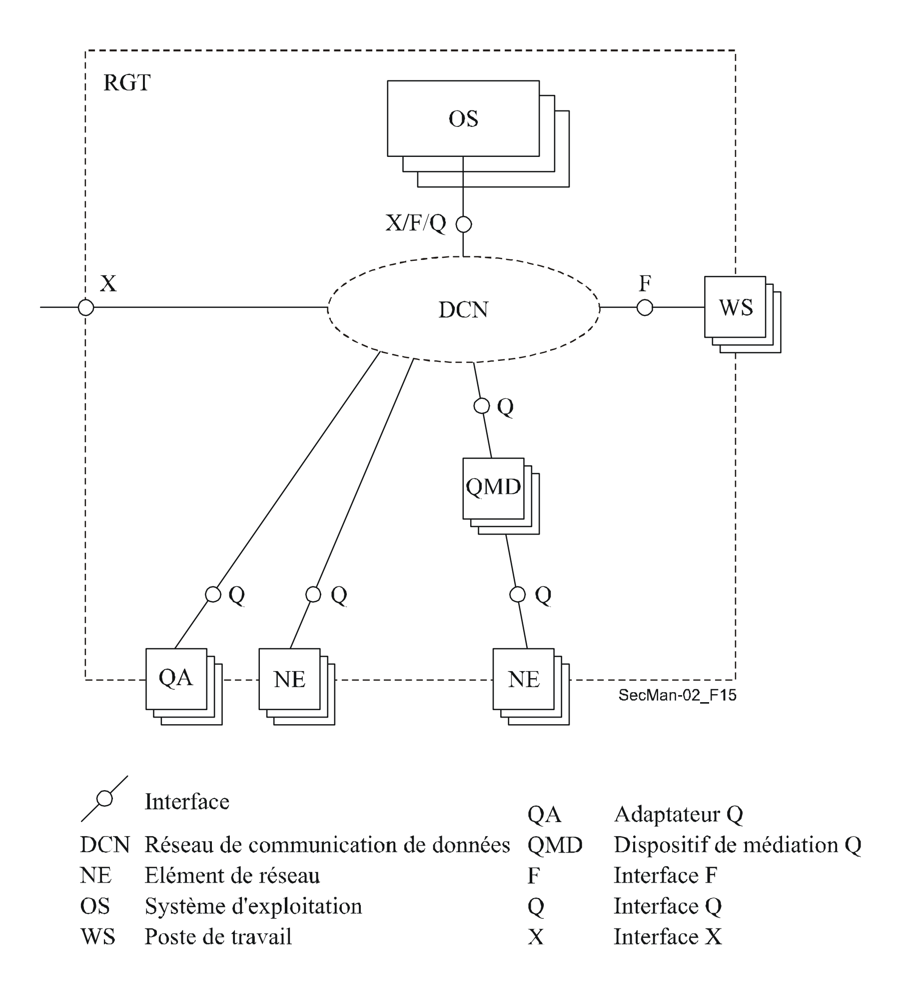


Figure 6-11 – Exemple d'architecture physique (M.3010)

Les exigences de sécurité varient d'une interface à l'autre. L'interface Q se trouve dans un seul domaine administratif tandis que l'interface X se trouve entre différents domaines administratifs qui peuvent appartenir à différents fournisseurs. Des services de sécurité sont nécessaires pour les deux interfaces, mais les contre-mesures requises pour l'interface X sont plus robustes. La Rec. UIT-T M.3016.0 fournit un aperçu général et un cadre qui identifient les menaces de sécurité concernant un RGT. Dans la série M.3016, la Rec. UIT-T M.3016.1 donne des détails sur les exigences de sécurité, la Rec. UIT-T M.3016.2 décrit les services de sécurité et la Rec. UIT-T M.3016.3 définit des mécanismes de sécurité permettant de faire face aux menaces dans le contexte de l'architecture fonctionnelle du RGT, décrite dans la Rec. UIT-T M.3010. Comme les exigences n'ont pas besoin d'être toutes prises en charge par les diverses organisations de normalisation, la Rec. M.3016.4 contient un formulaire permettant de créer des profils des exigences, des services et des mécanismes de sécurité, ces profils pouvant être utilisés pour assurer la conformité à la politique de sécurité propre à une organisation. La Rec. UIT-T M.3320 traite des aspects propres à l'interface X. Les aspects de protocole relatifs aux différentes couches de communication sont spécifiés dans les Rec. UIT-T Q.811 et Q.812.

Lorsqu'on examine la sécurité dans le contexte de la gestion, deux facettes sont à prendre en considération. La première concerne le plan de gestion pour une activité de bout en bout (par exemple services de téléphonie IP). L'activité de gestion consistant à administrer les utilisateurs doit être réalisée de manière sécurisée. On parle de *sécurité des informations de gestion* échangées sur le réseau pour le déploiement d'une application de bout en bout. La deuxième facette est la gestion des informations de sécurité. Quelle que soit l'application (par exemple téléphonie IP ou activité de signalisation de dérangement entre deux fournisseurs de services), des mesures de sécurité telles que l'utilisation de clés de chiffrement doivent aussi être gérées. On parle souvent de *gestion des informations de sécurité*. L'infrastructure PKI définie au paragraphe précédent est un exemple de cette facette. La Rec. UIT-T M.3400 définit un certain nombre de fonctions liées à ces deux facettes.

Sur la base du cadre défini dans la Rec. UIT-T X.805, plusieurs Recommandations portant sur des fonctions de gestion sont disponibles pour les trois cellules du plan de gestion (voir la Figure 2-1). Les paragraphes qui suivent illustrent certaines de ces Recommandations et montrent comment les besoins de sécurité sont pris en considération. En plus des Recommandations relatives aux trois cellules du plan de gestion, il en existe d'autres qui définissent des services génériques ou communs, par exemple l'envoi d'alarme en cas de violation de sécurité physique, des fonctions d'audit et des modèles d'information définissant des niveaux de protection pour différentes cibles (c'est-à-dire les entités de gestion).

6.4.2 Intersection du plan de gestion et de la couche infrastructure

Cette cellule concerne la sécurisation de l'activité de gestion des éléments d'infrastructure du réseau, à savoir les éléments de commutation et de transmission et les liaisons entre ces éléments ainsi que les systèmes d'extrémité tels que les serveurs. Les activités telles que la configuration d'un élément de réseau doivent par exemple être réalisées par un utilisateur autorisé. Une connectivité de bout en bout peut être envisagée en termes de réseaux d'accès et de réseaux centraux. Différentes technologies peuvent être employées dans ces réseaux. Des Recommandations ont été élaborées pour les deux types de réseau (réseau d'accès et réseau central). On prend ici l'exemple du réseau optique passif à large bande (BPON, *broadband passive optical network*) utilisé comme réseau d'accès. L'administration des privilèges des utilisateurs pour un tel réseau d'accès est définie au moyen de la méthodologie de modélisation unifiée dans la Rec. UIT-T Q.834.3 et l'échange de gestion utilisant l'architecture de courtier de requêtes pour objets communs (CORBA, *common object request broker architecture*) est spécifié dans la Rec. UIT-T Q.834.4. L'interface décrite dans ces Recommandations est l'interface Q illustrée sur la Figure 6-11. Elle est appliquée entre le système de gestion des éléments et le système de gestion du réseau. Le système de gestion des éléments sert à gérer les différents éléments de réseau et a donc connaissance des détails internes des architectures matérielle et logicielle des éléments d'un ou de plusieurs fournisseurs et le système de gestion du réseau réalise les activités au niveau du réseau de bout en bout et couvre les systèmes de gestion de plusieurs fournisseurs. La Figure 6-12 montre les divers objets utilisés pour créer, supprimer, attribuer et utiliser des informations de contrôle d'accès pour les utilisateurs du système de gestion des éléments. La liste de permissions des utilisateurs contient, pour chaque utilisateur autorisé, la liste des activités de gestion qui sont permises. Le gestionnaire de contrôle d'accès vérifie l'identité et le mot de passe de l'utilisateur de l'activité de gestion et autorise l'accès à la fonctionnalité figurant dans la liste de permissions.

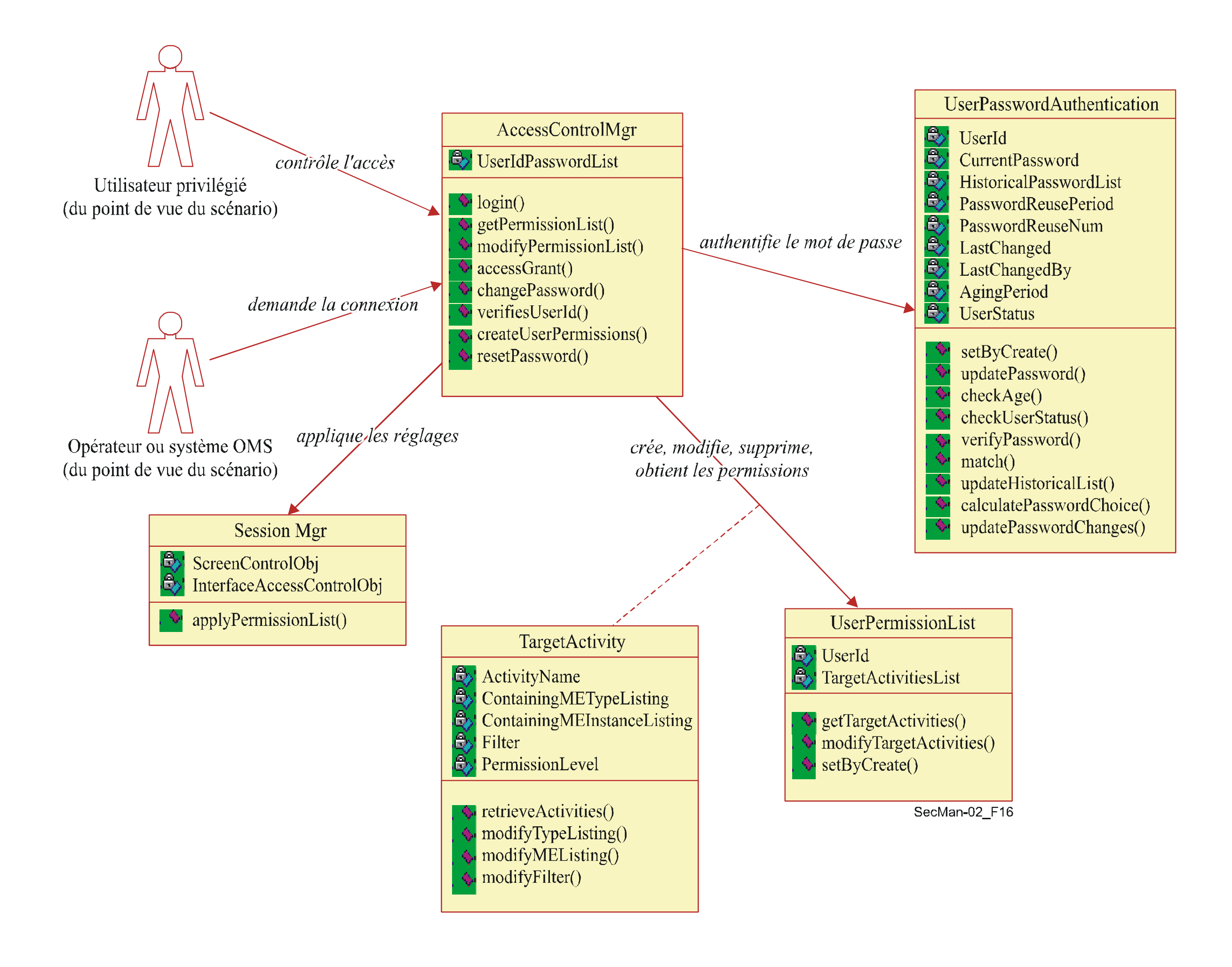


Figure 6-12 – Administration des privilèges des utilisateurs (Q.834.3)

6.4.3 Intersection du plan de gestion et de la couche services

L'intersection entre le plan de gestion et la couche services concerne la sécurisation des activités de surveillance et de contrôle des ressources de réseau configurées pour l'offre de services par le fournisseur de services. Les Recommandations de l'UIT-T portent sur deux aspects de cette intersection. Le premier aspect consiste à veiller à ce que des mesures de sécurité appropriées soient disponibles pour les services qui sont disponibles dans le réseau (par exemple veiller à ce que seuls des utilisateurs valables soient autorisés à exécuter les opérations associées à la fourniture d'un service). Le second aspect consiste à définir les échanges administratifs et de gestion qui sont valables. Cette définition facilitera la détection des violations de sécurité. En cas de violations de sécurité, celles-ci sont souvent gérées au moyen de systèmes de gestion spécifiques.

Un exemple de Recommandation portant sur le premier aspect, l'activité de gestion d'un service, est la Rec. UIT-T M.3208.2 sur la gestion de connexion. Un client du service de gestion de connexion qui possède des liaisons préconfigurées utilise ce service pour former une connexion par circuits loués de bout en bout. Ce service de gestion de connexion permet à un abonné de créer/activer, modifier et supprimer des circuits loués dans les limites des ressources préconfigurées. Comme l'utilisateur fournit

la connectivité de bout en bout, il est nécessaire de garantir que seuls les utilisateurs autorisés peuvent exécuter ces opérations. Les dimensions de sécurité définies pour l'activité de gestion associée à ce service font partie des huit dimensions examinées au § 2.4. Ce sont: authentification d'entité homologue, contrôle d'intégrité des données (afin d'empêcher toute modification non autorisée des données en transit) et contrôle d'accès (pour garantir qu'un abonné n'accède pas de façon malveillante ou accidentelle aux données d'un autre abonné).

La Rec. UIT-T M.3210.1 est un exemple de Recommandation qui définit les activités administratives associées au plan de gestion pour les services hertziens. Elle correspond au second aspect examiné ci-dessus.

Dans un réseau hertzien, lorsque les utilisateurs se déplacent entre leur réseau de rattachement et un réseau visité, ils peuvent traverser différents domaines administratifs. Les services définis dans la Rec. UIT-T M.3210.1 décrivent comment le domaine de gestion des fraudes du réseau de rattachement collecte les informations appropriées concernant un abonné une fois que celui-ci est enregistré dans un réseau visité. Les scénarios a) et b) de la Figure 6-13 illustrent le déclenchement de l'activité de gestion de surveillance respectivement par le réseau de rattachement et par le réseau visité. Le système de détection des fraudes du réseau de rattachement demande des informations sur les activités d'un abonné qui s'enregistre dans un réseau visité jusqu'à ce que cet abonné quitte le réseau ou annule son enregistrement dans ce réseau. Des profils d'utilisation peuvent alors être élaborés sur la base des relevés d'appel et de l'analyse au niveau du service ou pour un abonné. Le système de détection des fraudes peut ensuite procéder à une analyse et produire des alarmes appropriées pour les comportements frauduleux.

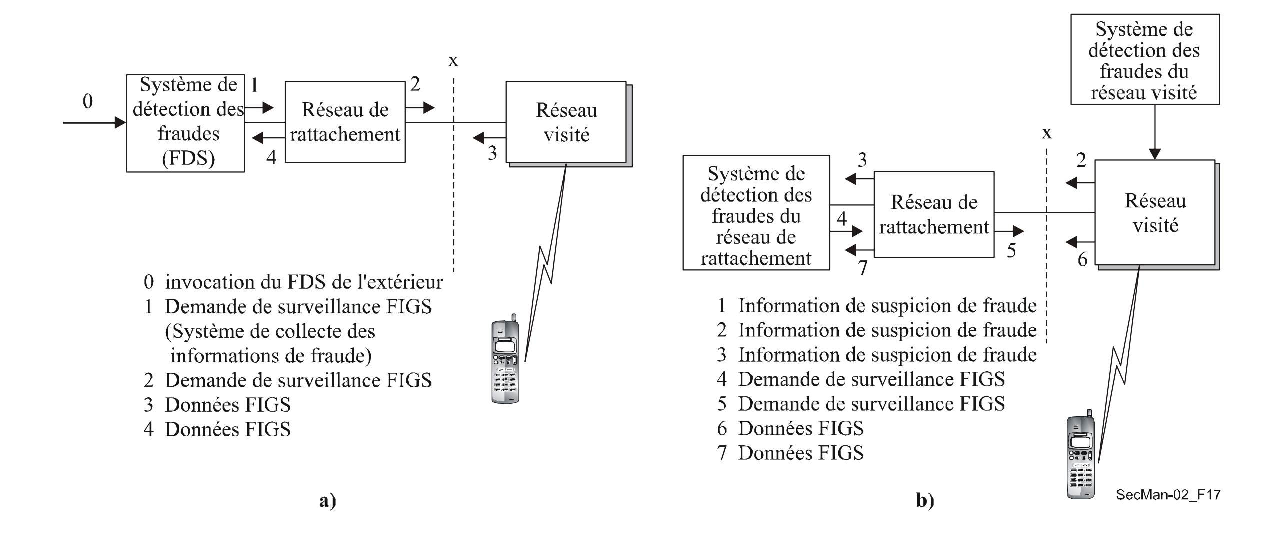


Figure 6-13 – Gestion des fraudes pour les services hertziens (Rec. UIT-T M.3210.1)

6.4.4 Intersection du plan de gestion et de la couche application

La troisième cellule, correspondant à l'intersection du plan de gestion et de la couche application, concerne la sécurisation des applications d'utilisateur final fondées sur le réseau. Les applications telles que la messagerie et les services d'annuaire sont définies dans les Recommandations des séries X.400 et X.500.

Une autre catégorie d'applications pour lesquelles les activités de gestion doivent être sécurisées correspond aux applications de gestion proprement dites. Cette déclaration, d'apparence obscure, sera mieux comprise à l'aide d'exemples. Pour ces applications, le personnel de gestion (d'exploitation) faisant partie de l'administration du fournisseur de service représente les utilisateurs finaux. Prenons le cas où un fournisseur de service utilise les services de connexion d'un autre fournisseur pour offrir un service de connectivité de bout en bout. Suivant l'environnement réglementaire ou le marché considéré, certains fournisseurs de services peuvent offrir des services d'accès et d'autres, appelés *opérateurs intercentraux*, peuvent offrir une connectivité longue distance. Les opérateurs intercentraux louent des services d'accès auprès du fournisseur local pour assurer la connectivité de bout en bout entre des endroits géographiques différents. En cas de perte de service, il est fait appel à une application de gestion appelée administration des dossiers de dérangement afin de signaler les dérangements entre systèmes de gestion. L'utilisateur de ces systèmes et de l'application proprement dite a besoin d'une autorisation pour pouvoir signaler des dérangements concernant les services. Les systèmes et utilisateurs autorisés doivent prendre les mesures qui s'imposent pour extraire l'état des dérangements signalés. La Figure 6-14 illustre les interactions qui doivent être réalisées de manière sécurisée. De manière analogue à l'administration des boîtes vocales pour l'application de messagerie électronique, les privilèges d'accès sont administrés afin d'éviter tout accès non autorisé aux dossiers de dérangement. Un fournisseur de services est autorisé à signaler uniquement des dérangements concernant les services qu'il loue et non des dérangements concernant les services loués par un fournisseur différent.

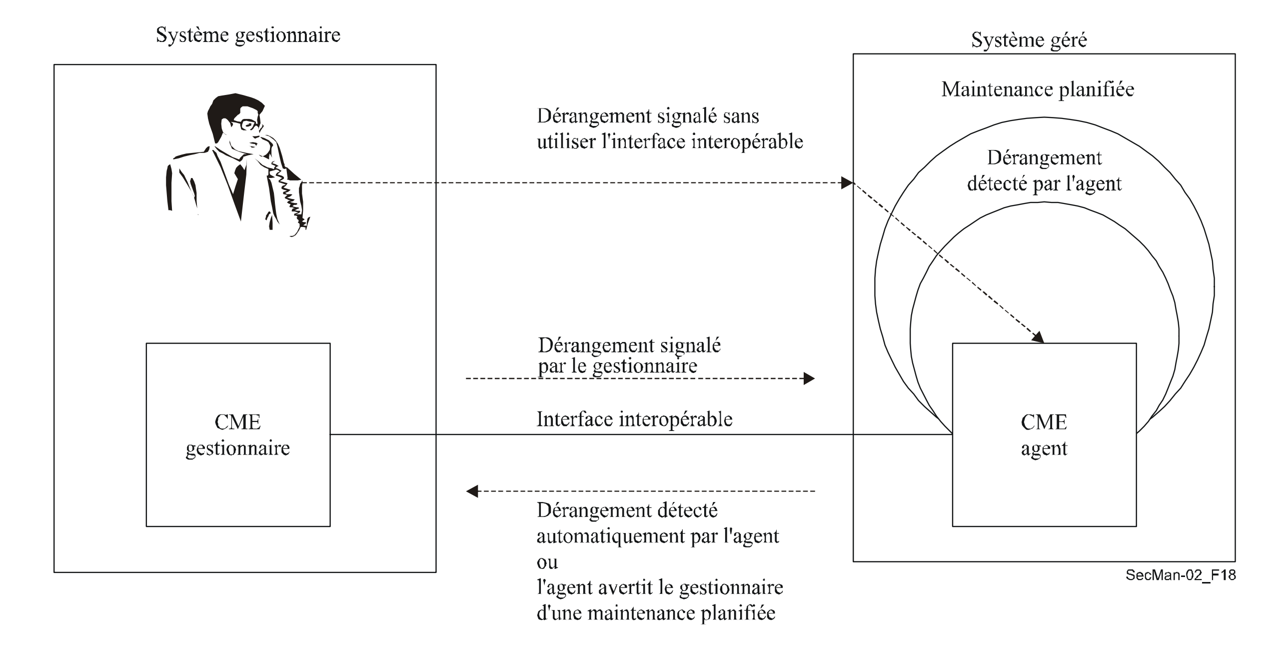


Figure 6-14 – Création d'un dossier de gestion de dérangement (Rec. UIT-T X.790)

La Rec. UIT-T X.790 définit cette application de gestion et utilise des mécanismes tels que la liste de contrôle d'accès et l'authentification bidirectionnelle pour sécuriser les activités. Cette application a été implémentée et déployée sur la base de cette Recommandation conjointement avec les mécanismes de sécurité applicables à l'authentification.

6.4.5 Services communs de gestion de la sécurité

Les Rec. UIT-T X.736, X.740 et X.741 définissent des services communs qui s'appliquent aux trois cellules du plan de gestion lorsque le protocole commun d'informations de gestion (CMIP, *common management information protocol*) est utilisé à l'interface. Les services définis dans ces Recommandations sont brièvement décrits ci-après. Il est à noter que toutes ces fonctions sont bien évidemment considérées comme correspondant à des activités dans le plan de gestion.

6.4.5.1 Fonction de signalisation des alarmes de sécurité: d'une manière générale, la signalisation des alarmes est une fonction essentielle dans les interfaces de gestion. Lorsqu'une défaillance est détectée, résultant d'un problème opérationnel (défaillance de l'ensemble de circuits) ou d'une violation de la politique de sécurité, une alarme est communiquée au système de gestion. Les rapports d'alarme incluent un certain nombre de paramètres, de sorte que le système de gestion puisse déterminer le motif de la défaillance et prendre une mesure corrective. Les paramètres relatifs à un événement donné incluent un champ obligatoire appelé type d'événement et un ensemble d'autres champs appelés informations d'événement. Ces derniers champs contiennent des informations telles que la gravité de l'alarme, les motifs probables de déclenchement de l'alarme, le détecteur de la violation de sécurité, etc. Les motifs de déclenchement des alarmes sont associés aux types d'événement comme indiqué dans le Tableau 6-2.

Tableau 6-2 – Motifs de déclenchement des alarmes de sécurité

Type d'événement	Motifs de déclenchement de l'alarme de sécurité
Violation de l'intégrité	Information dupliquée Information manquante Détection de modification d'information Information hors séquence Information inattendue
Violation opérationnelle	Refus de service Hors service Erreur de procédure Raison non spécifiée
Violation physique	Altération frauduleuse du câble Détection d'intrusion Raison non spécifiée
Violation de service ou de mécanisme de sécurité	Echec d'authentification Atteinte à la confidentialité Echec de non-répudiation Tentative d'accès non autorisée Raison non spécifiée
Violation du domaine temporel	Information tardive Mot de passe périmé Activité en dehors de l'horaire

On trouvera davantage d'explications sur ces motifs de déclenchement des alarmes dans la Rec. UIT-T X.736. Plusieurs de ces motifs ont trait aux menaces examinées dans des paragraphes précédents.

6.4.5.2 Fonction de journal d'audit de sécurité: pour qu'un gestionnaire de la sécurité puisse enregistrer les violations de sécurité et les conserver dans un journal d'audit, la Rec. UIT-T X.740 identifie un certain nombre d'événements à consigner dans un journal d'audit. Il s'agit des connexions, des déconnexions, des utilisations de mécanismes de sécurité, des opérations de gestion et de la comptabilisation de l'utilisation. Le modèle considéré utilise le mécanisme de journalisation défini dans la Rec. UIT-T X.735, un journal général pour enregistrer tous les événements produits au niveau du système géré. Dans le cadre de la fonction de journal d'audit, on définit deux événements se rapportant à des violations de sécurité: le rapport de service et le rapport d'utilisation. Le rapport de service concerne la fourniture, le refus ou la reprise d'un service. Le rapport d'utilisation sert à indiquer qu'un enregistrement contenant des données statistiques relatives à la sécurité a été créé. Comme pour chaque événement, un certain nombre de valeurs de motif ont été définies pour le rapport de service (par exemple demande de service, refus de service, échec de service, reprise de service, etc.). De nouveaux types d'événement pourront être définis si nécessaire car les deux types indiqués dans la Recommandation ne seront peut-être pas suffisants dans l'avenir.

6.4.5.3 La Rec. UIT-T X.741 définit de façon très détaillée le modèle associé à l'attribution d'un certain contrôle d'accès aux diverses entités gérées. Les définitions relatives au contrôle d'accès données dans cette Recommandation permettent notamment de satisfaire aux exigences suivantes: les informations de gestion sont protégées contre toute création, suppression et modification non autorisées, les opérations autorisées relatives aux entités sont compatibles avec les droits d'accès de ceux qui sont à l'origine des opérations et la transmission d'informations de gestion à des destinataires non autorisés est interdite. Divers niveaux de contrôle d'accès sont définis pour respecter les exigences susmentionnées. Pour les opérations de gestion, les dispositions énoncées dans la Recommandation facilitent la mise en place de restrictions d'accès à plusieurs niveaux: l'entité gérée dans son ensemble, les attributs de l'entité, les valeurs des attributs, le contexte de l'accès et les actions au niveau de l'entité. Un certain nombre de mécanismes tels qu'une liste de contrôle d'accès, fondée sur des capacités, fondée sur des étiquettes et fondée sur des contextes ont été définis et une politique de contrôle d'accès peut appliquer un ou plusieurs de ces mécanismes. Dans ce modèle fondé sur une politique et des informations de contrôle d'accès (ACI, *access control information*), une décision est prise concernant l'autorisation ou non de l'opération demandée. Les informations ACI sont par exemple constituées de règles, de l'identité du demandeur, des identités des cibles auxquelles l'accès est demandé, d'informations relatives à l'authentification du demandeur, etc. Le modèle est très riche en fonctionnalités et, dans une application donnée, les capacités peuvent ne pas être toutes requises.

6.4.5.4 Services de sécurité fondés sur l'architecture CORBA: tandis que les Recommandations UIT-T de la série X.700 reposent sur l'utilisation du protocole CMIP comme protocole aux interfaces de gestion, il existe d'autres tendances dans le secteur, visant à introduire l'utilisation d'un protocole, de services et de modèles d'objet fondés sur le courtier de requête pour objets communs pour les interfaces de gestion. La Rec. UIT-T Q.816 définit un cadre pour l'utilisation de ces services dans le contexte des interfaces de gestion. En ce qui concerne la prise en charge des exigences de sécurité pour ces interfaces, cette Recommandation renvoie à la spécification de l'OMG relative aux services de sécurité communs.

6.5 Ordonnances électroniques

La fourniture de soins de santé nécessite et génère une grande variété de données et d'informations, dont la collecte, le traitement, la distribution, l'accès et l'utilisation doivent se faire de façon sécurisée et dans le strict respect des règles éthiques et juridiques. Cela revêt un caractère crucial pour les données cliniques et les informations de gestion, mais est également important pour d'autres types d'informations telles que celles qui sont contenues dans les bases de données épidémiologiques, de littérature et de connaissances.

Les sources de ces types de données et d'informations se trouvent aussi bien à l'intérieur qu'à l'extérieur de l'infrastructure des soins de santé et sont situées à des distances variables de leurs utilisateurs respectifs. En pratique, les utilisateurs nécessitent et génèrent un mélange de ces types d'informations dans le cadre de leurs fonctions respectives, par exemple un médecin peut consulter une base de données de connaissances lorsqu'il examine un patient puis inclure des informations pertinentes dans le dossier du patient, qui peuvent ensuite être utilisées à des fins de facturation.

Les rencontres et les transactions en matière de soins de santé présentent de multiples facettes. Elles se produisent par exemple entre un patient et un médecin, entre deux médecins, entre un médecin généraliste et un médecin spécialiste, entre un patient et un établissement de santé tel qu'un laboratoire d'analyses, une pharmacie ou un centre de rééducation. Ces rencontres peuvent avoir lieu dans sa propre communauté, dans une autre partie du pays ou à l'étranger. Toutes ces rencontres nécessitent des données et des informations avant de commencer véritablement et génèrent des données et des informations en cours de rencontre ou peu après. Ces données et ces informations peuvent être de différentes tailles et être requises ou générées à différents moments et sous différentes formes, par exemple discours, nombres, texte, graphiques et images statiques ou dynamiques, et sont souvent un mélange judicieux de tous ces types.

Les sources et répertoires de ces données et informations peuvent se trouver dans différents endroits et prendre différentes formes, par exemple, dossiers complets des patients, ordonnances écrites à la main et rapports de médecins généralistes, de médecins spécialistes ou de laboratoires.

Traditionnellement, toutes ces rencontres se faisaient en tête-à-tête et les paroles et les écrits étaient les principaux modes utilisés pour les communications et pour l'archivage des dossiers médicaux, tandis que le transport était principalement assuré par des services publics ou privés par voie routière, ferrée ou aérienne. Au fur et à mesure de la croissance du réseau téléphonique, celui-ci est devenu le réseau de communication des professionnels et établissements de santé, à l'échelle nationale et internationale, jusqu'à l'émergence et à la croissance d'outils modernes de télématique pour la santé.

L'utilisation de technologies modernes dans les aspects cliniques/médicaux des services de soins de santé ne fait qu'augmenter et concerne les instruments et les équipements (notamment les équipements de détection et de mesure), les services de laboratoire, l'imagerie statique et dynamique. Compte tenu de la croissance de l'utilisation de ces technologies ainsi que de leur variété et de leur sophistication, il était inévitable que de nombreux services utilisant des technologies modernes se séparent des établissements de soins de santé traditionnels – se séparent sur le plan de la distance et de manière plus significative sur le plan de la gestion. Ainsi, les communications entre ces services utilisant des technologies modernes et les services de soins de santé traditionnels sont devenues importantes du point de vue de l'efficacité et de la rentabilité de ces services.

L'utilisation des technologies de l'information et des communications (TIC) par le secteur de la santé a commencé à se généraliser il y a plus de 25 ans avec la simple messagerie électronique qui permettait d'acheminer des notes et des rapports purement alphanumériques. Tout comme les communications téléphoniques ont constitué le principal motif de l'installation de téléphones dans les cabinets des médecins et dans les établissements de soins de santé, le courrier électronique a été la principale justification initiale de l'installation de liaisons de télécommunication modernes. Et, plus l'utilisation de la messagerie électronique s'est généralisée, plus les exigences en termes de qualité de fonctionnement et de couverture géographique se sont renforcées: davantage d'endroits à une vitesse plus grande et avec une plus grande largeur de bande pour pouvoir prendre en charge les pièces jointes de plus en plus volumineuses des messages électroniques. Au cours des dix dernières années, on a assisté à une croissance exponentielle de l'utilisation de la messagerie électronique dans le secteur de la santé, à l'échelle nationale et internationale, y compris dans les pays les plus pauvres, notamment sur l'Internet. Par exemple, les transactions électroniques sont devenues monnaie courante pour les fonctions qui n'exigent pas vraiment de rencontres en tête-à-tête, par exemple pour préparer et envoyer des ordonnances et des rapports, fixer des rendez-vous et programmer des services, adresser des patients à un confrère et, lorsque la qualité des services de télécommunication le permet, pour transmettre des images médicales accompagnées de leur interprétation écrite ou orale faite par un spécialiste.

Les TIC sont par ailleurs utilisées de façon complexe en télémédecine, qui est "la fourniture de soins médicaux par le biais de communications audio, vidéo et de données", y compris l'établissement effectif du diagnostic, l'examen voire l'apport de soins à un patient qui se trouve dans un endroit distant. La télémédecine est un domaine important qui prend de l'ampleur et qui devrait modifier bon nombre des approches traditionnelles en matière de soins de santé; de fait, c'est le point de départ d'un nouveau modèle pour les soins médicaux.

Un autre domaine qui n'est pas à proprement parler récent, mais qui s'élargira utilement avec la généralisation de la prise en charge de la télématique, est l'accès aux systèmes fondés sur la connaissance et leur utilisation. Ces systèmes, également appelés systèmes experts et systèmes d'appui aux décisions, sont des systèmes qui donnent des avis et conseils spécialisés sur des problèmes et procédures médico-scientifiques. Par exemple, à partir des coordonnées et des symptômes d'un patient, ces systèmes peuvent faciliter l'établissement du diagnostic, suggérer des analyses complémentaires ou proposer un traitement.

Toutes les évolutions susmentionnées ont également une grande incidence sur les systèmes d'informations de gestion (MIS, *management information system*) requis et utilisés dans le secteur de la santé, par exemple les systèmes MIS hospitaliers. Ceux-ci ne sont plus des systèmes destinés à la gestion administrative des soins hospitaliers prodigués aux patients, de l'admission au renvoi/transfert, mais incluent une multitude d'interfaces intelligentes et conviviales pour le personnel médical avec, par exemple, des systèmes d'appui aux décisions cliniques, des liaisons de télémédecine, des portails de sites web, etc.

Par ailleurs, il convient de citer deux caractéristiques des professionnels de santé à prendre en considération: leur mobilité et le besoin qu'ils ont d'avoir les mains libres et donc de pouvoir les utiliser pour les soins médicaux proprement dits. La caractéristique de mobilité signifie qu'ils peuvent accéder aux informations médicales requises (par exemple au dossier électronique d'un patient) ou à un outil ou à un instrument, à partir de n'importe quel endroit distant et chaque fois que c'est nécessaire sous réserve de leur vérification, que ce soit à l'intérieur d'un bâtiment ou d'une ville, mais aussi dans l'ensemble d'un pays ou à l'étranger. Et la caractéristique des mains libres signifie qu'il faut trouver des mécanismes d'identification et d'autorisation qui n'exigent pas d'intervention manuelle du professionnel médical, par exemple ouvrir une porte ou taper sur un clavier d'ordinateur.

Le secteur des soins de santé est donc un secteur fondé sur énormément d'informations, dans lequel la collecte, la circulation, le traitement, la présentation et la distribution de données et d'informations de santé ou liées à la santé, sont essentiels pour l'efficacité, l'efficience et la rentabilité du fonctionnement et du développement des services de soins de santé, à l'échelle nationale et internationale.

Il est extrêmement important que toute cette circulation se fasse de manière sécurisée et confidentielle, et dans le strict respect des règles et réglementations éthiques et juridiques.

6.5.1 Considérations relatives aux infrastructures PKI et PMI pour les applications de télésanté

Par le biais du chaînage des autorités de certification, l'infrastructure PKI reproduit une structure hiérarchique du monde réel, qu'il s'agisse d'une hiérarchie géopolitique (régions-pays-Etats-localités) ou thématique (santé-médecine-chirurgie-chirurgie spécialisée-fournisseurs, etc.). En outre, étant donné que le secteur de la santé est universel, hiérarchique, très important et de plus en plus interactif à l'échelle internationale, la définition d'une interface PKI/PMI normalisée pour la santé devient absolument nécessaire.

L'interopérabilité technique des systèmes de santé doit être garantie grâce à une large utilisation des normes techniques. La plupart des fournisseurs de solutions de sécurité ont déjà adopté des normes telles que la Rec. UIT-T X.509. L'authentification d'utilisateur étant une application critique qui dépend des informations locales, la liberté de choisir une infrastructure PKI/PMI donnée ne devrait pas avoir d'incidence sur la capacité de l'utilisateur d'interfonctionner avec des personnes certifiées par d'autres infrastructures PKI/PMI dans le secteur de la santé (qui, bien entendu, repose sur au moins un minimum de normalisation concernant les politiques de contrôle d'accès et d'autres politiques associées). Pour cela, différentes stratégies peuvent être mises en place, qui peuvent inclure la reconnaissance croisée des différentes infrastructures ou l'utilisation d'une racine commune. L'adoption de normes techniques, l'interopérabilité technique des différentes infrastructures et la normalisation de certaines politiques garantiront un environnement pleinement efficace et entièrement intégré pour les transactions en matière de santé dans le monde entier.

6.5.2 Système d'ordonnances électroniques de Salford

Le système d'ordonnances électroniques décrit dans le document [Policy] est un bon exemple d'infrastructures PKI et PMI appliquées à la télésanté. Compte tenu du grand nombre de professionnels impliqués dans le programme de transmission électronique des ordonnances (ETP, *electronic transmission of prescriptions*) au Royaume-Uni (34 500 médecins généralistes, 10 000 infirmières délivrant des ordonnances, nombre qui devrait passer à 120 000 au cours des prochaines années, 44 000 pharmaciens agréés et 22 000 dentistes) et des autorisations très peu nombreuses qui sont véritablement requises (c'est-à-dire les divers niveaux de permission concernant la délivrance des ordonnances et des médicaments et l'accès à la gratuité des médicaments), le système de contrôle

d'accès en fonction des prérogatives (RBAC, *role-based access control*) semble constituer le mécanisme d'autorisation idéal à utiliser pour le programme ETP. Lorsqu'on prend également en considération le nombre de patients potentiels au Royaume-Uni (60 millions) et le fait que les médicaments obtenus gratuitement représentent 85% des médicaments prescrits [*FreePresc*], le système RBAC devrait aussi être utilisé pour contrôler l'accès à la gratuité des médicaments si possible. Compte tenu du grand nombre de professionnels qui doivent être autorisés et du grand nombre de patients dont l'accès à la gratuité des médicaments doit être accordé, il est essentiel de répartir la gestion des rôles entre autorités compétentes plutôt que d'essayer de la centraliser, faute de quoi le système deviendrait ingérable.

Chaque professionnel dépend d'un organe officiel qui lui donne le droit d'exercer. Au Royaume-Uni, le General Medical Council est chargé d'enregistrer les médecins et de les radier en cas de faute professionnelle. Le General Dental Council remplit une fonction analogue pour les dentistes, le Nursing and Midwifery Council pour les infirmières et le Royal College of Pharmacy pour les pharmaciens. Dans le système ETP susmentionné, ces organes sont chargés de l'attribution des rôles, puisqu'ils s'acquittent déjà parfaitement bien de cette fonction.

Créé en juin 2001, le ministère du travail et des retraites (DWP, *Department for work and pensions*) a remplacé les anciens ministères de la sécurité sociale et de l'enseignement et de l'emploi. Il est chargé de verser les allocations de chômage et les retraites et, conjointement avec l'autorité de tarification des ordonnances (PPA, *prescription pricing authority*), de déterminer les bénéficiaires de la gratuité des médicaments. Ces bénéficiaires sont nombreux: personnes de 60 ans et plus, enfants de moins de 16 ans, adolescents de 16, 17 ou 18 ans qui sont scolarisés à temps complet, personnes ou leur conjoint recevant une allocation de soutien du revenu ou une allocation de demandeur d'emploi, personnes titulaires d'un certificat HC2 (*low income scheme full help certificate*) dans le cadre du système de santé national (NHS, *national health system*), femmes enceintes, les femmes ayant accouché au cours des 12 derniers mois et personnes recevant une pension d'invalidité de guerre. La gestion de ces bénéficiaires est donc répartie entre différentes branches du DWP et de la PPA.

Un certificat d'attribut de rôle est attribué à chaque professionnel par l'organe dont il dépend et il est enregistré dans l'annuaire LDAP de cet organe. Le système ETP pourra prendre des décisions concernant l'autorisation de délivrer des ordonnances ou des médicaments s'il a accès à ces annuaires LDAP. De même, si le DWP attribue des certificats d'attribut de rôle aux personnes bénéficiant de la gratuité des médicaments pour diverses raisons et qu'il les enregistre dans son ou ses annuaires LDAP, le système ETP pourra prendre des décisions concernant l'accès à la gratuité des médicaments en accédant à ces annuaires LDAP, et le pharmacien n'aura pas à demander au patient la preuve qu'il bénéficie de cette gratuité. Cette preuve ne sera nécessaire que lorsqu'un patient fait nouvellement partie des bénéficiaires, par exemple lorsque la grossesse d'une femme vient tout juste d'être diagnostiquée par son médecin généraliste et que le DWP n'a pas eu le temps de créer le certificat d'attribut officiel.

Ces rôles sont ensuite utilisés par un moteur de décision (tel que PERMIS, voir www.permis.org), qui détermine si des médecins sont autorisés à délivrer des ordonnances, des pharmaciens à délivrer des médicaments et des patients à bénéficier de la gratuité des ordonnances, conformément à la politique ETP. Chaque application ETP (système pour la délivrance des ordonnances, système pour la délivrance des médicaments et système PPA) lit la politique ETP au moment de l'initialisation puis, lorsqu'un professionnel demande une action (par exemple délivrer une ordonnance ou des médicaments), le moteur de décision extrait le rôle de la personne dans l'annuaire LDAP approprié et prend une décision conformément à la politique. Les utilisateurs peuvent donc accéder à de multiples applications et tout ce dont ils ont besoin d'avoir est une paire de clés PKI. L'émission des certificats d'attribut de rôle peut avoir lieu sans que l'utilisateur n'intervienne et les utilisateurs n'ont pas à se soucier de savoir comment et où ces certificats sont enregistrés et utilisés par le système.

La Figure 6-15 contient un exemple d'implémentation d'un système d'ordonnances électroniques au Royaume-Uni, qui illustre plusieurs problèmes de sécurité essentiels qui se posent au moment de l'implémentation. Le cœur du système est constitué par une infrastructure de sécurité qui assure non seulement une forte authentification (à savoir une infrastructure PKI utilisant des certificats de clé

publique) mais aussi une forte autorisation (à savoir une infrastructure PMI) qui permet de donner une autorisation aux professionnels médicaux sur la base de leurs rôles enregistrés dans les certificats d'attribut. Les modèles classiques utilisent des listes de contrôle d'accès enfouies dans chaque application particulière (par exemple dossiers médicaux, bases de données d'ordonnances, assurance, etc.), pouvant obliger les utilisateurs (médecins, pharmaciens, patients, etc.) à obtenir et à administrer plusieurs jetons de sécurité différents (par exemple nom d'utilisateur/mot de passe, carte, etc.). Dans le nouveau modèle qui intègre les architectures PKI et PMI, l'utilisateur n'a besoin que d'un seul jeton – le certificat de clé publique de l'utilisateur – pour accéder aux différents services et aux différentes ressources qui sont réparties géographiquement ou topologiquement. Les certificats d'attribut de l'utilisateur sont conservés dans le système et non par l'utilisateur et sont transférés d'un composant à un autre en fonction des souhaits afin d'accorder un accès. Comme les certificats d'attribut sont signés numériquement par leurs émetteurs, ils ne peuvent pas être altérés au cours de ces transferts.

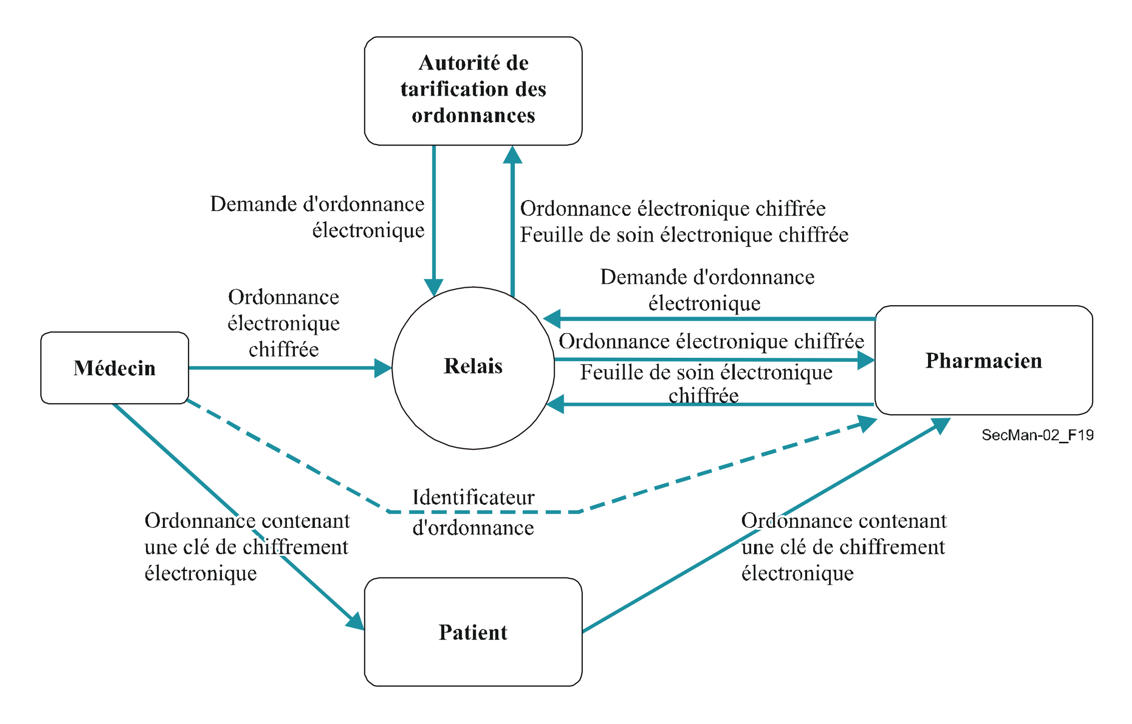


Figure 6-15 – Système d'ordonnances électroniques de Salford

Dans l'exemple de la Figure 6-15, des ordonnances électroniques sont créées par le médecin, signées numériquement (à des fins d'authentification), soumises à un chiffrement symétrique au moyen d'une clé de session aléatoire (à des fins de confidentialité), puis envoyées à une unité de stockage centrale. Le patient reçoit une ordonnance papier sur laquelle figure un code barre contenant la clé de chiffrement symétrique. Il se rend ensuite à la pharmacie de son choix et remet l'ordonnance au pharmacien, qui scanne le code barre, extrait l'ordonnance et la déchiffre. C'est le patient qui, en fin de compte, a la maîtrise de la personne qui est autorisée à lui délivrer les médicaments, comme dans le système actuel fonctionnant avec des ordonnances papier. Mais ce n'est pas suffisant. Il faut également prévoir des contrôles concernant les personnes autorisées à prescrire tel ou tel médicament et les personnes autorisées à les délivrer et concernant les personnes bénéficiant de la gratuité des médicaments.

Même si la description ci-dessus fait apparaître un système fortement intégré, celui-ci peut en réalité être réparti. En effet, l'annuaire d'attributs des médecins peut être différent du système qui authentifie les pharmaciens ou qui stocke les droits et politiques en matière de délivrance de médicaments, etc., qui s'appuient sur des tiers de confiance pour authentifier et autoriser les différents acteurs. Même si la mise en œuvre de solutions propriétaires est envisageable pour les infrastructures PKI et PMI, le recours à des solutions normalisées (par exemple la Rec. UIT-T X.509) permet aujourd'hui d'offrir un accès plus généralisé et global aux ordonnances électroniques.

6.6 Communications mobiles sécurisées de données de bout en bout

Les terminaux mobiles dotés de capacités de communication de données (téléphone mobile IMT-2000, ordinateur personnel portable, PDA avec carte radio, etc.) sont très répandus, et divers services d'application (par exemple commerce électronique mobile) destinés aux terminaux raccordés au réseau mobile apparaissent. S'agissant de commerce électronique, la sécurité est nécessaire et même indispensable.

De nombreux aspects liés à la sécurité du point de vue de l'opérateur mobile sont à l'étude (par exemple, architecture de sécurité des réseaux téléphoniques mobiles IMT-2000). Toutefois, il importe également de s'intéresser au point de vue de l'utilisateur mobile et à celui du fournisseur de services d'application (ASP, *application service provider*).

En ce qui concerne la sécurité des communications mobiles du point de vue de l'utilisateur mobile ou du fournisseur de services d'application, l'un des aspects les plus importants est celui de la sécurité des données transmises de bout en bout entre un terminal mobile et un serveur d'application.

En outre, pour ce qui est du système mobile connectant un réseau mobile à un réseau ouvert, il est nécessaire de s'intéresser à la sécurité dans les couches supérieures (couches Application, Présentation et Session) du modèle de référence OSI, car il existe diverses implémentations possibles de réseau mobile (par exemple, réseau téléphonique mobile IMT-2000, réseau local hertzien, Bluetooth) ou de réseau ouvert.

6.6.1 Cadre général des technologies de sécurité pour les communications mobiles de données de bout en bout

La Rec. UIT-T X.1121 décrit des modèles de communications mobiles sécurisées de données de bout en bout entre des terminaux mobiles et des serveurs d'application dans les couches supérieures. Deux types de modèles de sécurité sont définis dans le cadre général de sécurité pour les communications mobiles de données de bout en bout entre un utilisateur mobile et un fournisseur ASP: un modèle général et un modèle avec passerelle. Un utilisateur mobile utilise le terminal mobile pour accéder à divers services mobiles offerts par des fournisseurs ASP. Un fournisseur ASP fournit un service mobile aux utilisateurs mobiles par le biais d'un serveur d'application. La passerelle de sécurité mobile sert de relais pour les paquets entre les terminaux mobiles et le serveur d'application et convertit un protocole de communication fondé sur le réseau mobile en un protocole fondé sur un réseau ouvert, et inversement.

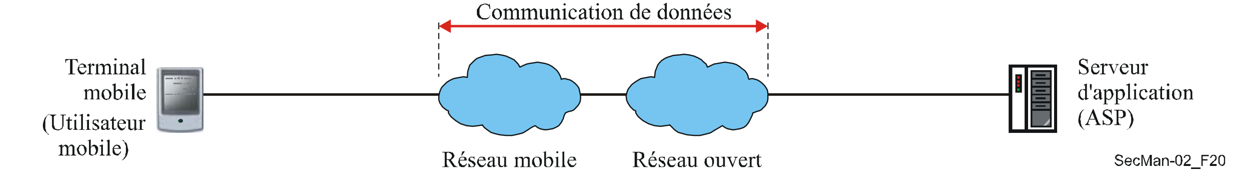


Figure 6-16 – Modèle général pour les communications mobiles de données de bout en bout entre un utilisateur mobile et un ASP

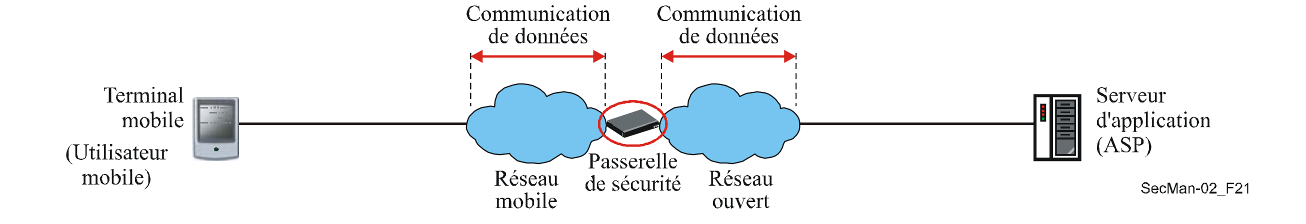


Figure 6-17 – Modèle avec passerelle pour les communications mobiles de données de bout en bout entre un utilisateur mobile et un ASP

La Rec. UIT-T X.1121 décrit aussi les menaces de sécurité concernant les communications mobiles de données de bout en bout ainsi que les exigences de sécurité du point de vue de l'utilisateur mobile et du point de vue du fournisseur ASP dans les deux modèles. Il existe deux catégories de menaces: d'une part les menaces générales présentes dans tout réseau ouvert et d'autre part les menaces propres au contexte mobile. La Figure 6-18 illustre les menaces présentes dans un réseau de communications mobiles de données de bout en bout.

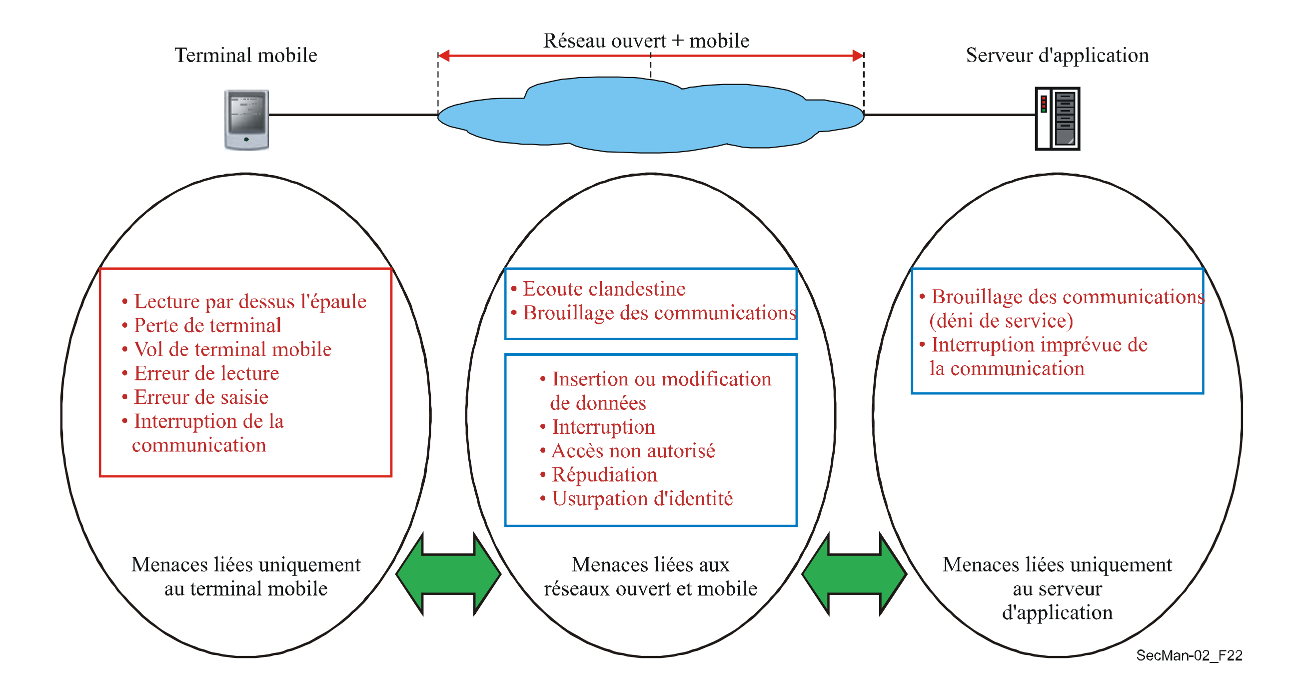


Figure 6-18 – Menaces concernant les communications mobiles de bout en bout

En outre, la Rec. UIT-T X.1121 précise les emplacements où les technologies de sécurité sont implémentées, lorsque c'est nécessaire pour chaque entité, et la relation entre les entités participant à une communication mobile de données de bout en bout (voir la Figure 6-19).

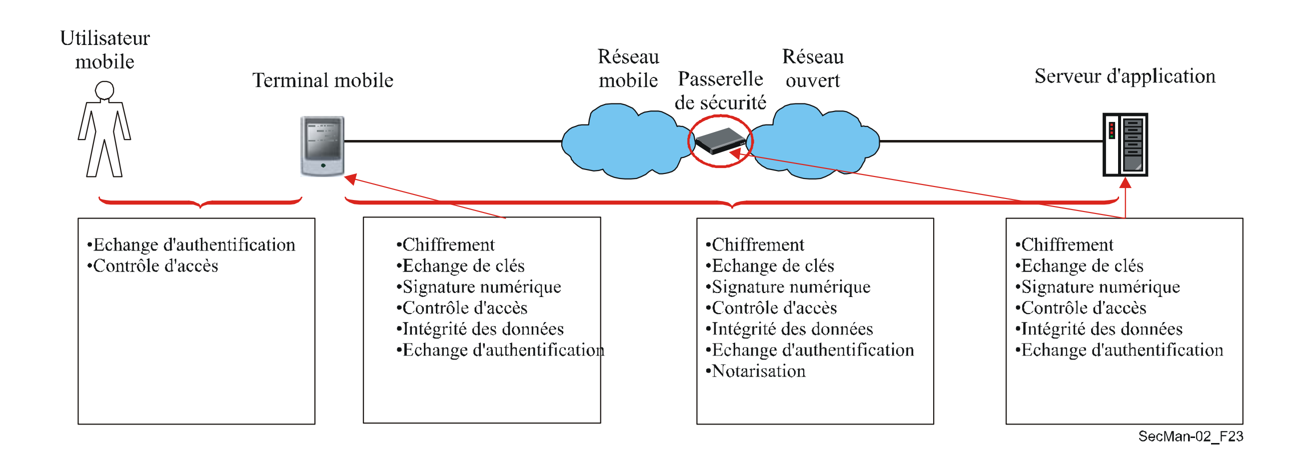


Figure 6-19 – Fonction de sécurité requise pour chaque entité et relation entre les entités

6.6.2 Considérations relatives à l'architecture PKI pour les communications mobiles sécurisées de données de bout en bout

Le présent paragraphe se rapporte à la Rec. UIT-T X.1122. La technologie PKI est très utile pour la protection des communications mobiles de données de bout en bout, mais certaines caractéristiques propres aux communications mobiles de données peuvent nécessiter une adaptation de la technologie PKI lors de l'élaboration de systèmes mobiles sécurisés. Deux types de modèles PKI ont été définis pour assurer des services de sécurité sur le trajet des communications mobiles de bout en bout. L'un est un modèle PKI général, dans lequel aucune fonction de passerelle de sécurité n'est présente sur le trajet d'une communication mobile de données de bout en bout, l'autre est un modèle PKI avec passerelle, dans lequel une passerelle de sécurité sert d'interface avec le réseau mobile et le réseau ouvert. La Figure 6-20 illustre le modèle PKI général pour les communications mobiles de bout en bout. Il comporte quatre entités. L'autorité de certification (CA, *certification authority*) de l'utilisateur mobile délivre un certificat à l'utilisateur mobile et gère le dépôt servant au stockage de la liste de révocation de certificats (CRL, *certificate revocation list*) qu'elle a déjà dressée. L'autorité de validation de l'utilisateur mobile (VA, *validation authority*) fournit un service de validation de certificat en ligne à l'utilisateur mobile. L'autorité de certification du fournisseur ASP délivre un certificat au fournisseur de services d'application et gère le dépôt servant au stockage de la liste de révocation de certificats qu'il a déjà dressée. L'autorité de validation du fournisseur ASP assure un service de validation de certificat en ligne pour les certificats de fournisseur ASP.

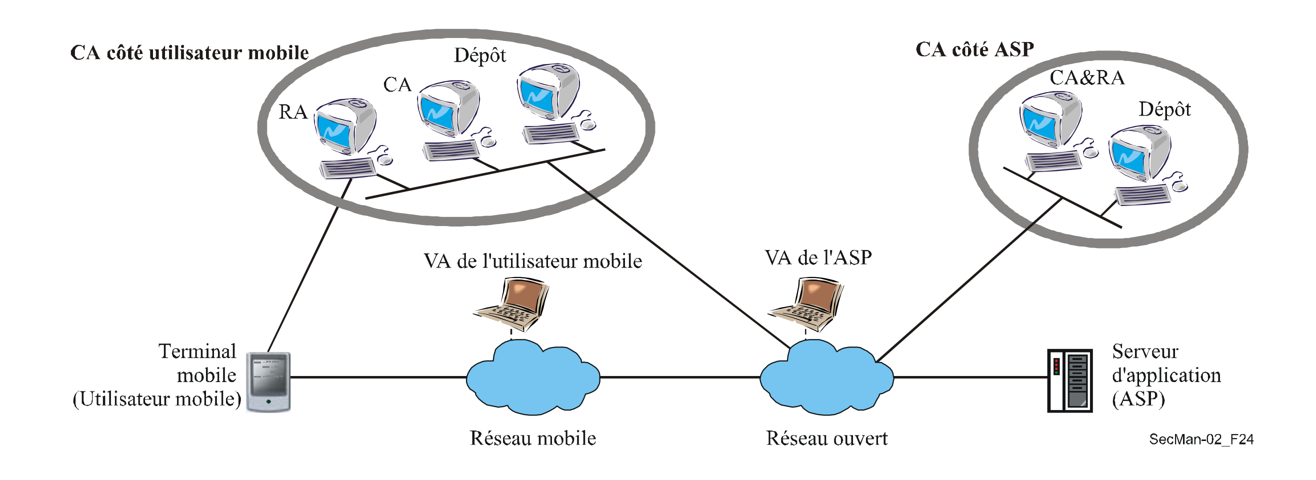


Figure 6-20 – Modèle PKI général pour les communications mobiles de données de bout en bout

Il existe deux méthodes de délivrance de certificat suivant l'endroit où les clés publique/privée sont produites. Dans la première méthode, la paire de clés de chiffrement est produite dans l'usine de fabrication du terminal mobile; dans la deuxième méthode, la paire de clés de chiffrement est produite dans le terminal mobile ou dans le jeton infraudable (carte à puce par exemple) rattaché au terminal mobile. La Figure 6-21 illustre la procédure d'acquisition de certificat par le terminal mobile sur la base de la procédure de gestion de certificat, lorsque la paire de clés de chiffrement est produite dans le terminal mobile.

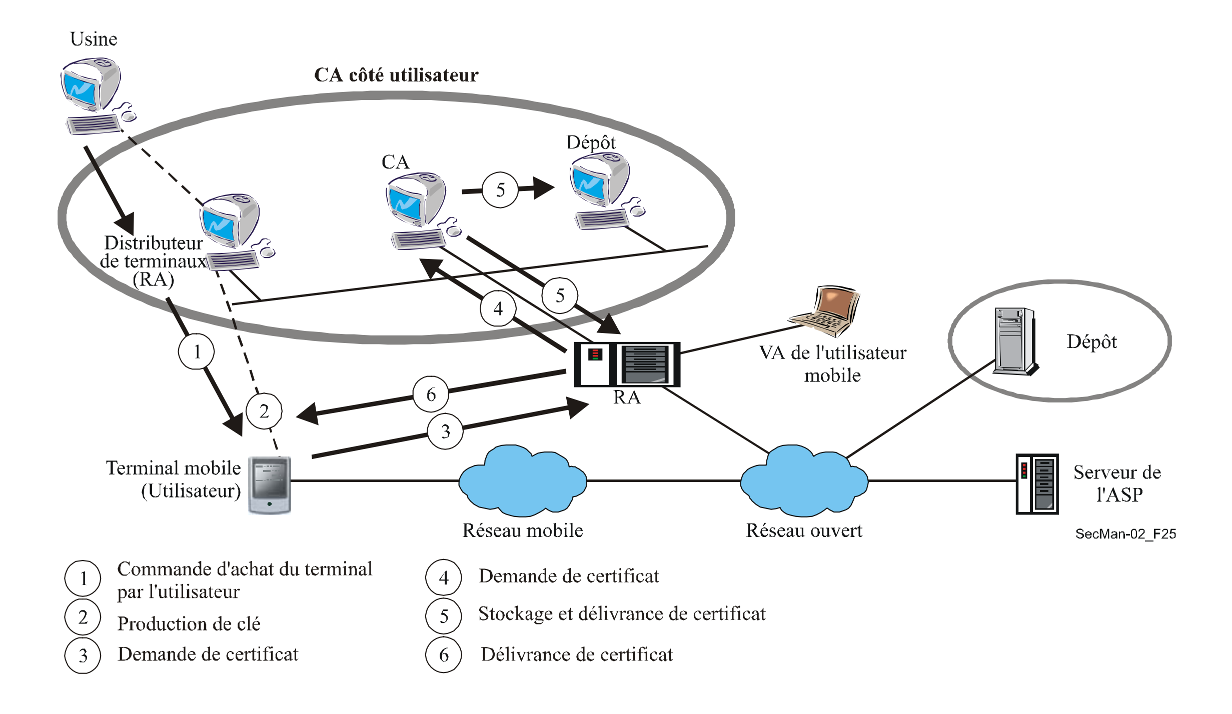


Figure 6-21 – Procédure de délivrance de certificat pour le terminal mobile

Le terminal mobile dispose d'une puissance de calcul et d'une taille de mémoire limitées. Par conséquent, il est préférable de procéder à une validation de certificat en ligne plutôt qu'à une validation de certificat hors ligne sur la base de la liste CRL. Lorsque le terminal mobile reçoit la paire message-signature avec la chaîne du certificat et qu'il souhaite vérifier la validité de la signature, le certificat devrait être utilisé après que la validité du certificat a été vérifiée au moyen de la méthode de validation de certificat. La Figure 6-22 illustre la procédure de validation de certificat en ligne pour le terminal mobile.

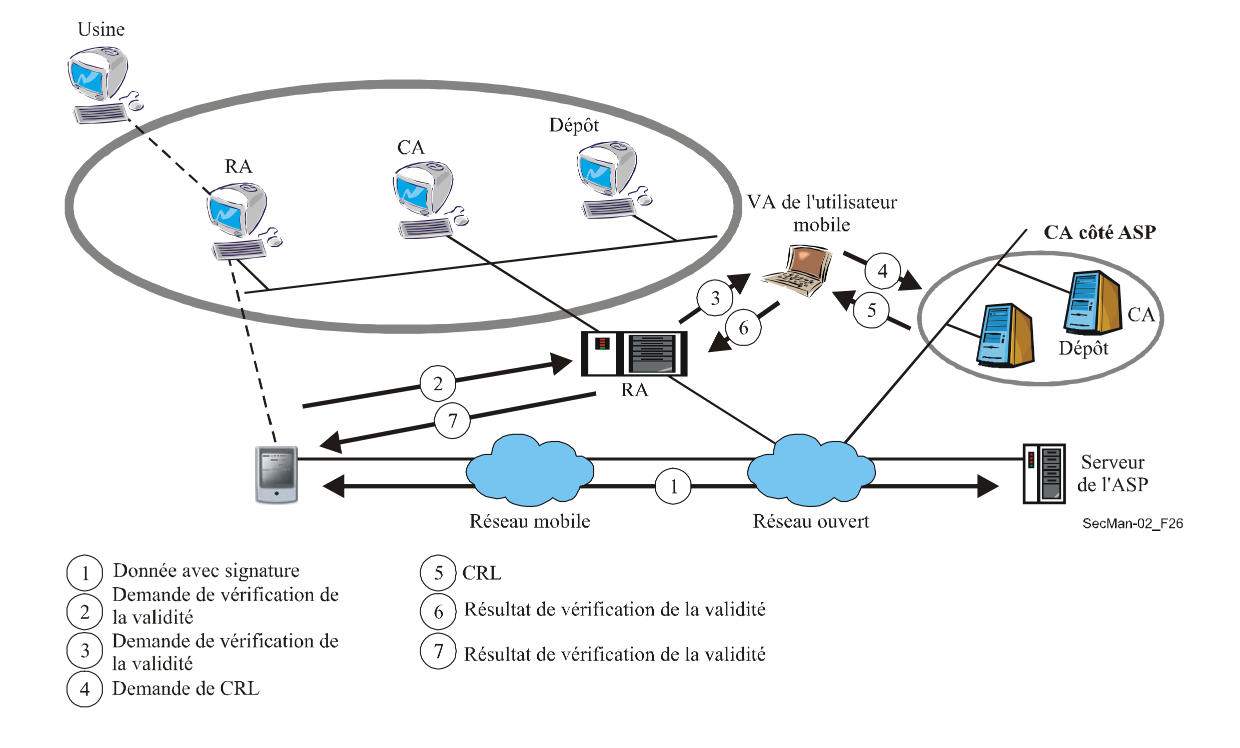


Figure 6-22 – Procédure de validation de certificat pour les communications mobiles de données de bout en bout

Le système PKI pour les communications mobiles de bout en bout peut être utilisé dans le cadre de deux modèles: l'un pour la couche session et l'autre pour la couche application. Le modèle pour la couche session assure des services de sécurité tels que l'authentification de client, l'authentification de serveur, la confidentialité et l'intégrité. Le modèle pour la couche application assure un service de non-répudiation et un service de confidentialité pour les communications mobiles de données de bout en bout.

En conclusion, la Rec. UIT-T X.1122 contient des considérations pour l'élaboration de systèmes mobiles sécurisés fondés sur l'infrastructure PKI du point de vue suivant: interopérabilité avec le système existant fondé sur l'infrastructure PKI dans un réseau ouvert, utilisation de l'infrastructure PKI dans l'environnement mobile (problèmes de production de clés, problèmes de demande et de délivrance de certificat, problèmes d'utilisation de certificat et problèmes liés aux autorités de certification) et considérations générales relatives à l'infrastructure PKI (problèmes de gestion du cycle de vie des certificats). Cette Recommandation peut servir de guide lors de l'élaboration de systèmes mobiles sécurisés fondés sur la technologie PKI.

7 Dimension disponibilité et couche infrastructure

Dans la Rec. UIT-T X.805, présentée au § 2:

- les dimensions de sécurité sont un ensemble de mesures de sécurité conçues pour tenir compte d'un aspect particulier de la sécurité du réseau; et
- les couches de sécurité correspondent à une hiérarchie de groupes de fonctionnalités et d'équipements de réseau auxquels les dimensions de sécurité s'appliquent.

La dimension de sécurité disponibilité permet de garantir qu'il n'y a pas déni de l'accès autorisé aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau. Les solutions de récupération en cas de catastrophe sont comprises dans cette catégorie.

La couche de sécurité infrastructure comprend les installations de transmission de réseau et les différents éléments de réseau protégés par les dimensions de sécurité. Elle représente les composants fondamentaux des réseaux, leurs services et applications. Elle comprend notamment les routeurs, commutateurs et serveurs ainsi que les liaisons de communication qui les relient.

Les exigences en termes de fonction, d'implémentation et d'exploitation spécifiées par l'UIT-T par rapport aux concepts susmentionnés sont nombreuses et variées. Elles concernent, entre autres, la qualité en termes d'erreurs, la limitation des encombrements, la signalisation des défaillances et les mesures correctives. Le présent paragraphe décrit différents points de vue sur les exigences liées aux réseaux de télécommunications afin de limiter les risques d'indisponibilité des ressources de transmission et d'en réduire les conséquences.

Afin de permettre à un opérateur de réseau de télécommunication de choisir une topologie de réseau appropriée par rapport aux objectifs de disponibilité, une référence à l'Annexe A de la Rec. UIT-T G.827 (*Exemples de topologies de conduit et de calculs de performance en termes de disponibilité de bout en bout*) est proposée.

7.1 Topologies de conduit et calculs de disponibilité de conduit de bout en bout

Les Figures 7-1 et 7-2 représentent les topologies de base de conduit qui peuvent être élaborées à partir des éléments de conduit prédéfinis.

La Figure 7-1 représente un conduit de base simple sans protection et la Figure 7-2 représente ce même conduit de base auquel a été ajouté un conduit de protection de bout en bout qui devrait emprunter un itinéraire distinct pour que la protection soit optimale.

On appelle cette forme de protection la configuration 1+1. Chacun des deux conduits est une connexion bidirectionnelle, le signal d'émission en provenance de chaque extrémité étant connecté en permanence aux deux conduits et un dispositif de commutation étant présent au niveau de chaque récepteur pour sélectionner le meilleur signal.

Une configuration plus économique consiste à utiliser un conduit de protection pour assurer la protection de plusieurs autres conduits. C'est ce qu'on appelle la configuration 1:n, qui nécessite des commutateurs de sélection au niveau des émetteurs et des récepteurs.

Pour les calculs de disponibilité de bout en bout, il est plus pratique d'utiliser le taux d'indisponibilité. L'Annexe A de la Rec. UIT-T G.827 énonce quelques principes de base pour évaluer la disponibilité dans le cas d'un conduit de base simple (Figure 7-1), dans le cas d'une topologie de protection de bout en bout 1+1 (Figure 7-2) et dans le cas d'une topologie avec un rapport de protection 1:n.

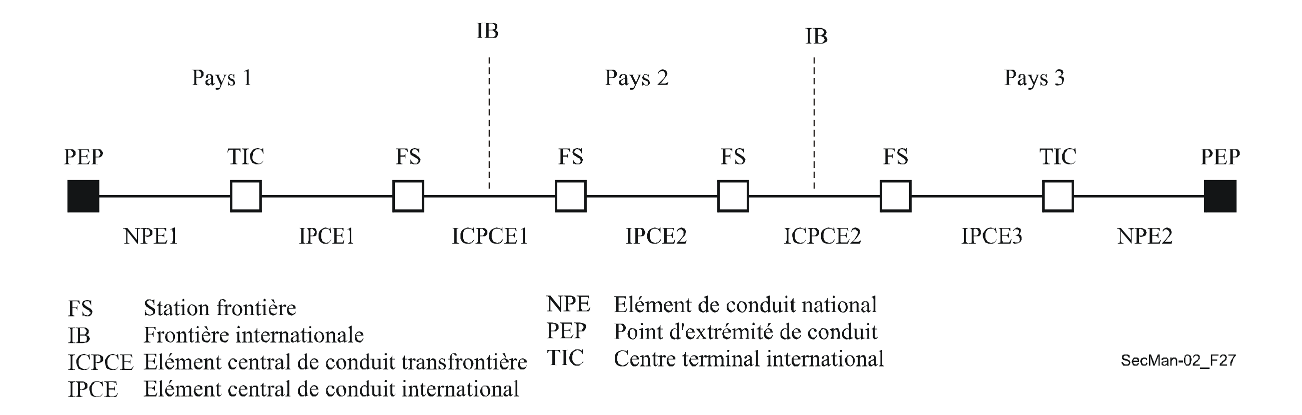


Figure 7-1 – Exemple de conduit de base simple sans protection

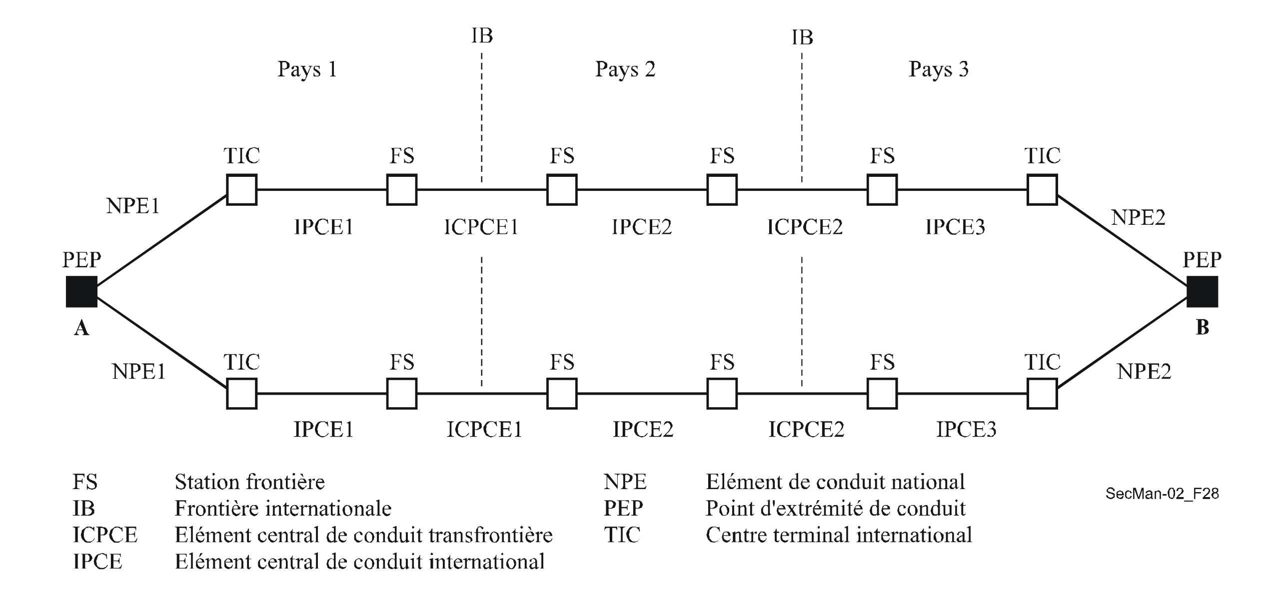


Figure 7-2 – Exemple de conduit avec protection de bout en bout

Le § 7.3 porte sur des topologies plus complexes, par exemple une topologie SDH (hiérarchie numérique synchrone) en anneau, dans laquelle le trafic peut être réacheminé en contournant une liaison en dérangement mais l'itinéraire de protection dépend des capacités de commutation des divers nœuds se trouvant sur l'anneau et n'est pas nécessairement la distance la plus courte entre deux nœuds. Pour ces topologies plus complexes, il est relativement difficile d'évaluer la disponibilité. Plusieurs publications citées dans l'Appendice I/G.827 abordent la question.

7.2 Amélioration de la disponibilité d'un réseau de transport – Aperçu

Les § 7.2 à 7.4 décrivent les caractéristiques architecturales des méthodes les plus couramment utilisées pour améliorer la disponibilité d'un réseau de transport. L'amélioration est obtenue par le remplacement des entités de transport ayant subi une défaillance ou une dégradation par d'autres entités spécialisées ou partagées. Le remplacement a normalement lieu à la suite de la détection d'un défaut, d'une dégradation de la qualité de fonctionnement ou d'une demande externe (par exemple gestion de réseau).

Protection – utilisation d'une capacité préassignée entre nœuds. L'architecture la plus simple possède une entité de protection dédiée pour chaque entité en service (protection 1+1). L'architecture la plus complexe possède m entités de protection partagées entre n entités en service (protection m:n). La commutation de protection peut être unidirectionnelle ou bidirectionnelle. En commutation de protection bidirectionnelle, la commutation concerne les deux sens de trafic, même si la défaillance n'affecte qu'un seul sens. En commutation de protection unidirectionnelle, la commutation ne concerne que le sens de trafic affecté, dans le cas d'une défaillance n'affectant qu'un seul sens.

Rétablissement – utilisation de toute capacité disponible entre nœuds. En général, les algorithmes utilisés pour le rétablissement impliquent un reroutage. Lorsque le rétablissement est utilisé, un certain pourcentage de la capacité du réseau de transport est réservé au reroutage du trafic normal.

La Rec. UIT-T G.805 contient des informations fondamentales sur ces aspects.

7.3 Protection

La disponibilité de service ne peut être élevée que si l'infrastructure de réseau est caractérisée par une grande fiabilité et une grande capacité de survie. Ainsi, si un équipement tombe en panne, il faut pouvoir commuter sur une autre source du signal (canal de protection).

Il existe deux types de protection. La *protection des équipements* est caractérisée par la présence d'ensembles de circuits redondants. Ainsi, en cas de panne matérielle sur un ensemble de circuits, une commutation est automatiquement opérée sur un autre ensemble de circuits. La *protection du réseau* permet d'assurer une protection contre les coupures de fibres en faisant passer le signal par d'autres conduits, dédiés ou partagés. Ces mécanismes sont illustrés sur la Figure 7-3.

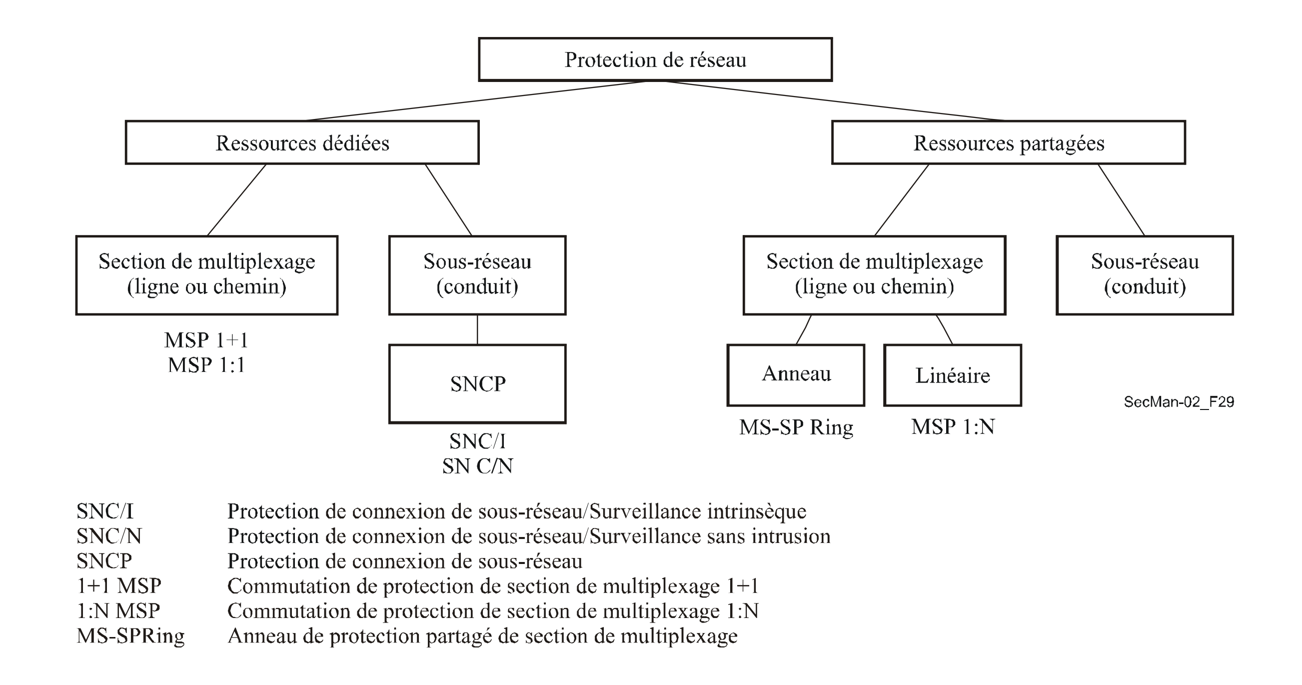


Figure 7-3 – Variantes de commutation de protection

Les mécanismes de protection peuvent être unidirectionnels ou bidirectionnels. Ils peuvent aussi être réversibles ou irréversibles. Ces termes sont définis dans la Rec. UIT-T G.780/Y.1351.

La *protection unidirectionnelle* est définie comme suit: "pour un dérangement unidirectionnel (c'est-à-dire un dérangement affectant un seul sens de transmission), seul le sens affecté (du chemin, de la connexion de sous-réseau, etc.) fait l'objet d'une commutation". Ainsi, seule une décision locale côté récepteur (nœud local) est prise et il n'est pas tenu compte de l'état du nœud distant pour procéder à la commutation de protection. Autrement dit, dans le cas d'une défaillance unidirectionnelle (c'est-à-dire une défaillance affectant un seul sens de transmission), seul le sens affecté fait l'objet d'une commutation de protection.

La *protection bidirectionnelle* est définie comme suit: "pour un dérangement unidirectionnel, les deux sens (du chemin, de la connexion de sous-réseau, etc.), à savoir le sens affecté et le sens non affecté, font l'objet d'une commutation". Ainsi, il est tenu compte à la fois de l'état local et de l'état distant pour procéder à la commutation de protection. Autrement dit, dans le cas d'une défaillance unidirectionnelle (c'est-à-dire une défaillance affectant un seul sens de transmission), les deux sens, à savoir le sens affecté et le sens non affecté, font l'objet d'une commutation de protection.

Le *fonctionnement (de protection) réversible* est défini comme suit: "en fonctionnement réversible, le signal de trafic (service) revient (ou reste) toujours au niveau de la connexion de sous-réseau/du chemin en service lorsque les requêtes de commutation sont terminées, c'est-à-dire lorsque la connexion de sous-réseau/le chemin en service est rétabli après le défaut ou lorsque la requête externe est relevée". Ainsi, en mode de fonctionnement réversible, le signal présent sur le canal de protection est recommuté sur le canal en service lorsque celui-ci est rétabli après le dérangement.

Le *fonctionnement (de protection) irréversible* est défini comme suit: "en fonctionnement irréversible, le signal de trafic (service) ne revient pas à la connexion de sous-réseau/au chemin en service lorsque les requêtes de commutation sont terminées". Ainsi, en mode de fonctionnement irréversible (applicable uniquement aux architectures 1+1), lorsque le canal en service défaillant est réparé, on maintient la sélection du signal de trafic normal ou protégé à partir du canal de protection.

Les formes de protection les plus courantes sont les suivantes:

- MSP 1:1 (commutation de protection de section de multiplexage 1:1, voir § 7.3.1)
- MSP 1+1 (commutation de protection de section de multiplexage 1+1, voir § 7.3.2)
- MS-SPRing (anneau de protection partagé de section de multiplexage, voir § 7.3.3)
- SNCP (protection de connexion de sous-réseau, voir § 7.3.4)

Ces mécanismes de protection vont être examinés plus en détail. Toutefois, un ensemble commun de Recommandations de référence s'applique: G.841 (caractéristiques), G.842 (interfonctionnement), G.783 (modèles fonctionnels), G.806 (défauts) et G.808.1 (commutation de protection générique).

7.3.1 Commutation de protection de section de multiplexage 1:1

Le diagramme de réseau est illustré sur la Figure 7-4.

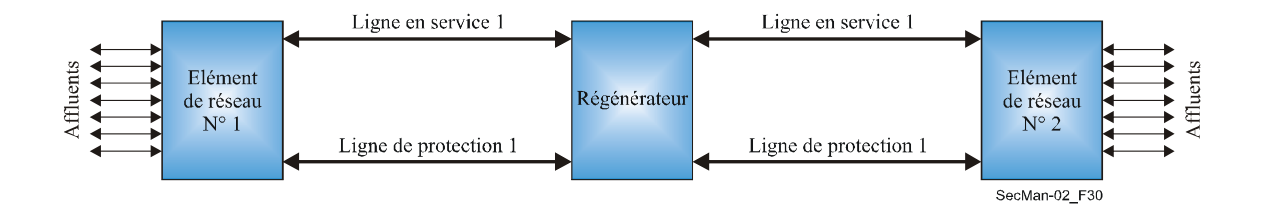


Figure 7-4 – Diagramme de réseau pour la commutation de protection 1:1

En commutation de protection 1:1, il existe un canal de protection pour chaque canal en service. Le canal de protection peut acheminer un autre trafic qui peut faire l'objet d'une préemption.

Un diagramme de l'intérieur d'un élément de réseau est illustré sur la Figure 7-5.

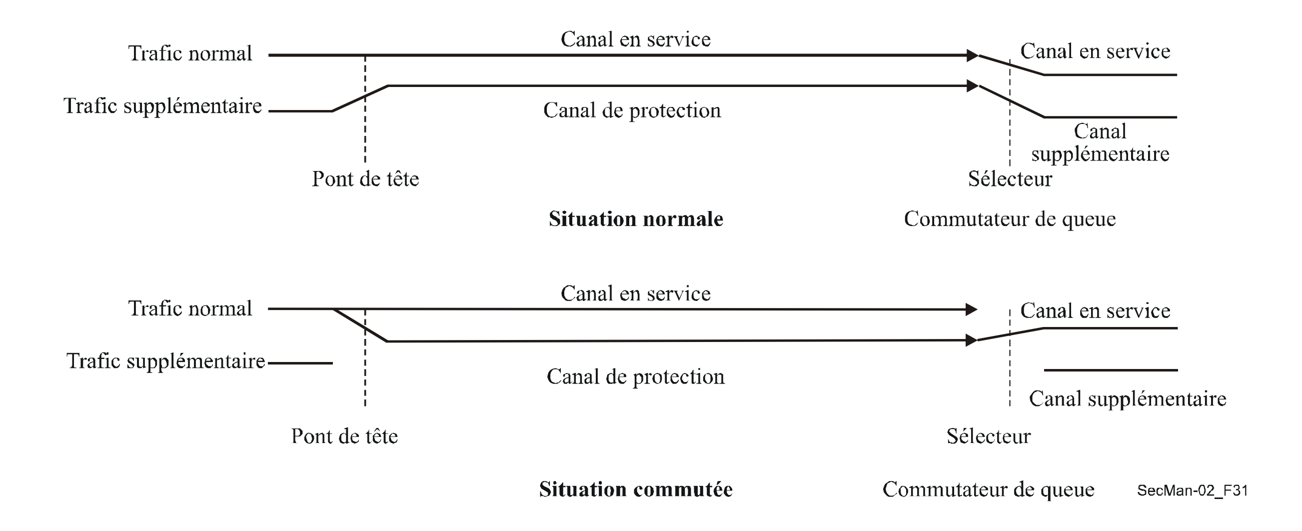


Figure 7-5 – Protection linéaire de section de multiplexage 1:1

En situation normale, un "trafic supplémentaire" peut être acheminé sur le canal de protection. Toutefois, si les octets K1/K2 corrects sont reçus (activant la fonction de protection), le "trafic normal" est ponté sur le canal de protection au niveau de la "tête" et commuté au niveau de la "queue". La commande est exécutée au moyen des octets K1 et K2 sur le canal de protection.

Cela correspond à une protection de ligne au niveau du module de transport synchrone de niveau N (niveau STM-N ($N \geq 1$)).

Les conditions à l'origine d'une commutation sont la commutation forcée et un certain nombre de situations de défaut ou de défaillance (par exemple signal de défaillance, perte de signal, perte de trame, erreurs excessives, signal de dégradation). On trouvera davantage de détails dans la Rec. UIT-T G.806.

7.3.2 Commutation de protection de section de multiplexage 1+1

Le diagramme de réseau est illustré sur la Figure 7-6.

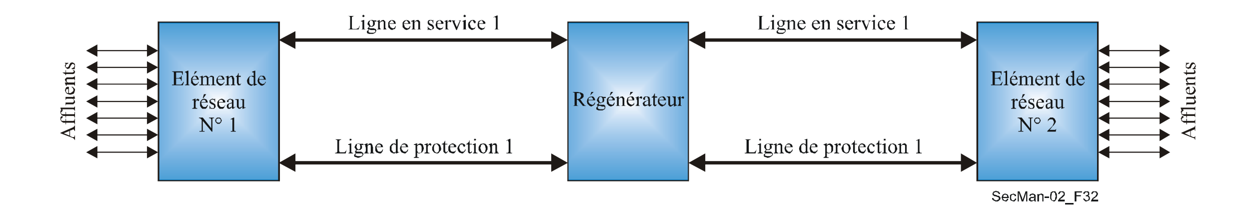


Figure 7-6 – Diagramme de réseau pour la commutation de protection 1+1

En commutation de protection 1+1, il existe un canal de protection pour chaque canal en service. Le canal de protection achemine une copie du signal acheminé sur le canal en service.

Un diagramme de l'intérieur d'un élément de réseau est illustré sur la Figure 7-7.

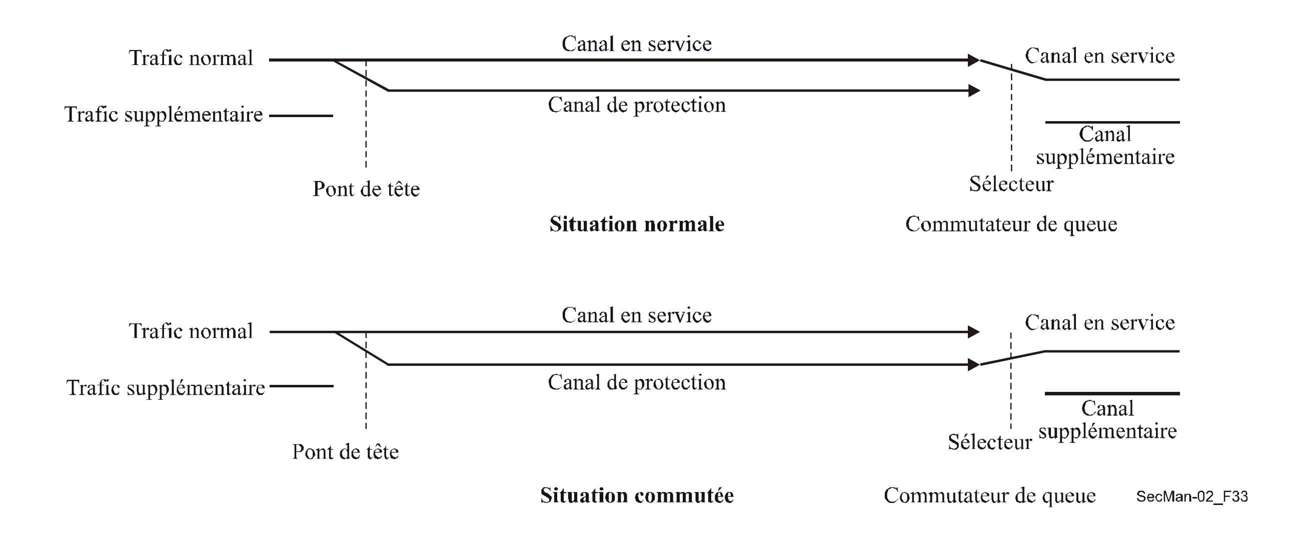


Figure 7-7 – Protection linéaire de section de multiplexage 1+1

Le signal émis est ponté en permanence sur la ligne de protection. Le récepteur sélectionne le meilleur signal.

Un mécanisme de protection 1+1 ne comporte pas de capacité de "trafic supplémentaire". Il permet d'assurer une fonction de protection de ligne. Il ne fonctionne donc qu'avec des modules STM-n, quel que soit le débit de la ligne. Il peut être considéré comme faisant partie de la catégorie de commutation de protection 1:1. Il n'a pas besoin de mécanisme de commande (octets K1 et K2 de commutation de protection automatique (APS, *automatic protection switching*) du surdébit de section de multiplexage (MSOH, *multiplex section overhead*)) pour fonctionner. La commutation est fondée sur les mêmes conditions de dérangement que celles indiquées au § 7.3.1.

Il existe une version de ce mécanisme de protection appelée mécanisme bidirectionnel 1+1, dans lequel les sélecteurs aux deux extrémités procèdent à une commutation. Ce mécanisme nécessite la transmission d'une commande au moyen des octets K1/K2.

7.3.3 Commutation de protection MS-SPRing

Le diagramme de réseau est illustré sur la Figure 7-8.

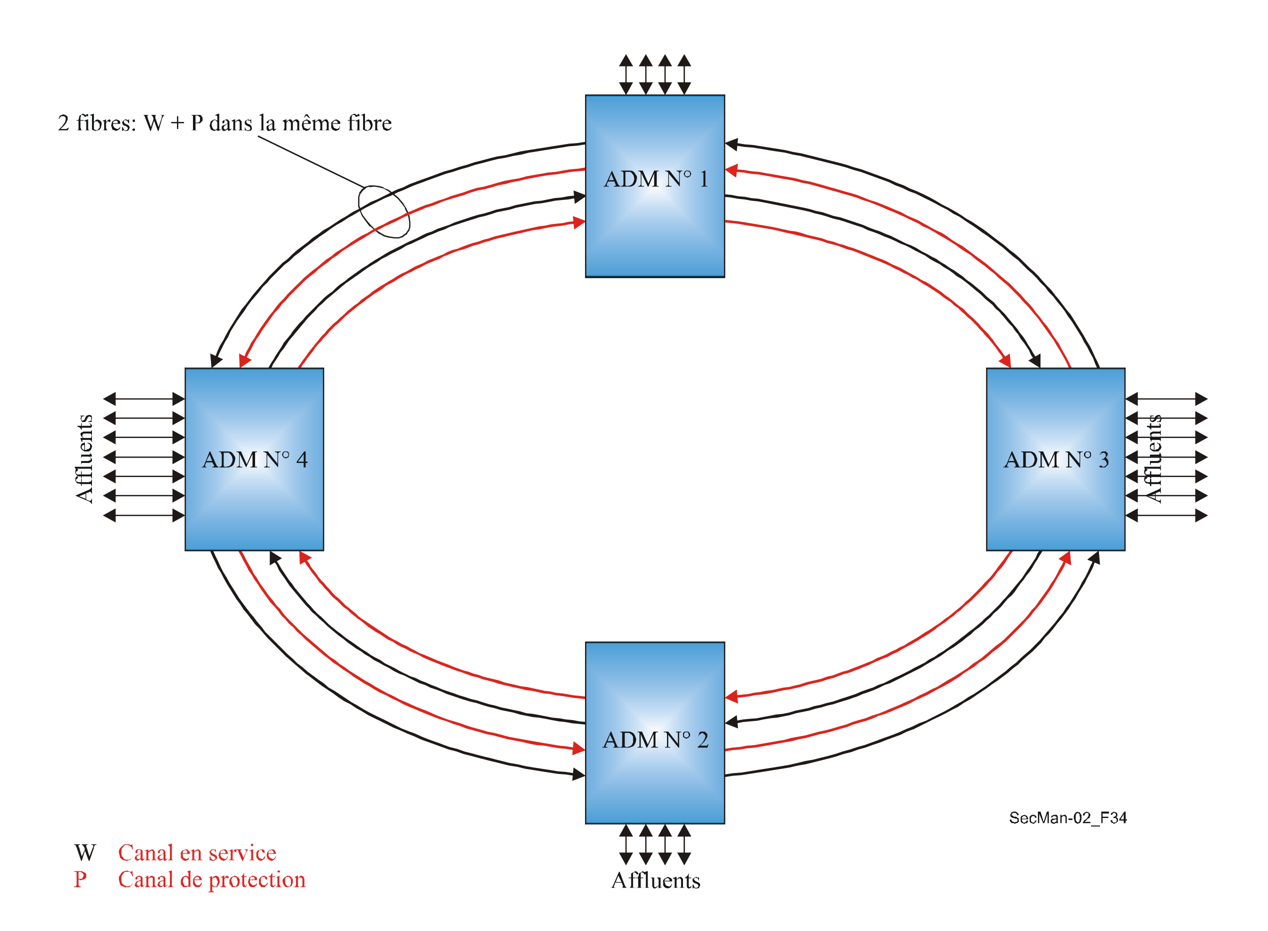


Figure 7-8 – Diagramme de réseau pour la commutation de protection MS-SPRing

La configuration MS-SPRing à deux fibres est la configuration dominante dans les réseaux SDH. Chaque tronçon de l'anneau comporte deux fibres, chacune acheminant la moitié de la largeur de bande des canaux en service et de protection (par exemple ligne STM-64 avec unités administratives (AU, *administrative unit*) AU-4 de 1 à 32 pour les canaux en service et AU-4 de 33 à 64 pour les canaux de protection). La protection du trafic normal acheminé sur les canaux en service sur une fibre est assurée par les canaux de protection dans le sens inverse.

La fonction MS-SPRing à deux fibres est illustrée sur la Figure 7-9.

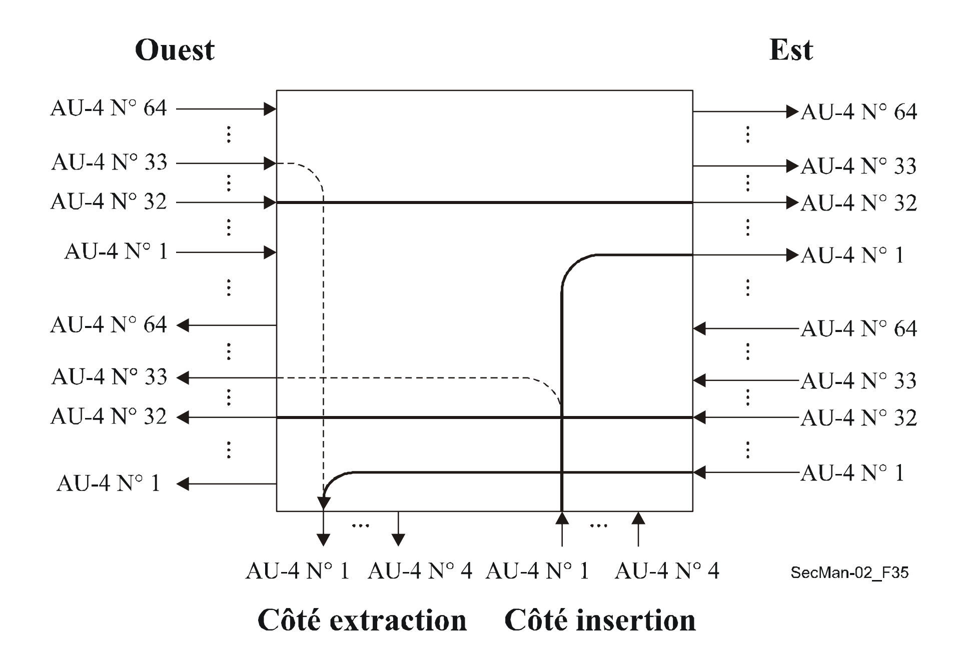


Figure 7-9 – Anneau STM-64 avec insertion-extraction STM-4

Sur la Figure 7-9, le signal constitutif "AU-4 N° 1 insertion" est transféré vers "émission AU-4 N° 1 est". Il est extrait de "réception AU-4 N° 1 est" vers "AU-4 N° 1 extraction". Il existe aussi une connexion directe pour l'unité AU-4 N° 32 représentée sur la Figure 7-9.

En cas de rupture de la fibre est, le signal "AU-4 N° 1 insertion" doit être transmis vers la protection côté ouest ("émission AU-4 N° 33 ouest") et le signal de réception doit être extrait de la protection côté ouest ("réception AU-4 N° 33 ouest") vers "AU-4 N° 1 extraction". L'unité AU-4 N° 32 provenant de l'ouest doit être bouclée sur l'unité AU-4 N° 64, l'unité AU-4 N° 32 provenant de l'est étant bouclée sur le canal de protection (AU-4 N° 64) de l'autre côté de la rupture. Ainsi, à ce nœud, la protection ("réception AU-4 N° 64 ouest") doit être bouclée sur le canal en service (AU-4 N° 32).

La commutation de protection est réalisée au niveau de la granularité AU-4 ou AU-3 pour tous les signaux acheminés sur la fibre. Les demandes et acquittements sont transmis au moyen des octets K1 et K2 de commutation de protection automatique (APS) du surdébit de section de multiplexage (MSOH). K1 et K2 sont transmis sur la ligne qui achemine les canaux de protection. Ils sont transmis dans les deux sens (est et ouest), le trajet étant court dans un sens et long dans l'autre sens.

Une suppression du signal est opérée afin d'éviter une fourniture du trafic au mauvais client dans le cas de l'isolement ou de la défaillance d'un nœud avec du trafic d'insertion/extraction (services provenant du même intervalle de temps mais sur des tronçons différents). On trouvera une description de la suppression du signal à l'Appendice II/G.841.

Les dérangements relatifs au signal de défaillance et au signal de dégradation sont les mêmes que dans le cas de la commutation de protection linéaire (voir § 7.3.1).

Trois configurations de commutation sont à envisager:

- normale (pas de dérangement);
- dérangement côté est (nécessité d'un bouclage à l'ouest et uniquement insertion/extraction depuis l'ouest);
- dérangement côté ouest (nécessité d'un bouclage à l'est et uniquement insertion/extraction depuis l'est);
- commutation de tronçon pour la protection MS-SPRing à 4 fibres (commutation sur l'entité de protection, pas de bouclage).

7.3.4 Commutation de protection SNCP

Le diagramme de réseau est illustré sur la Figure 7-10.

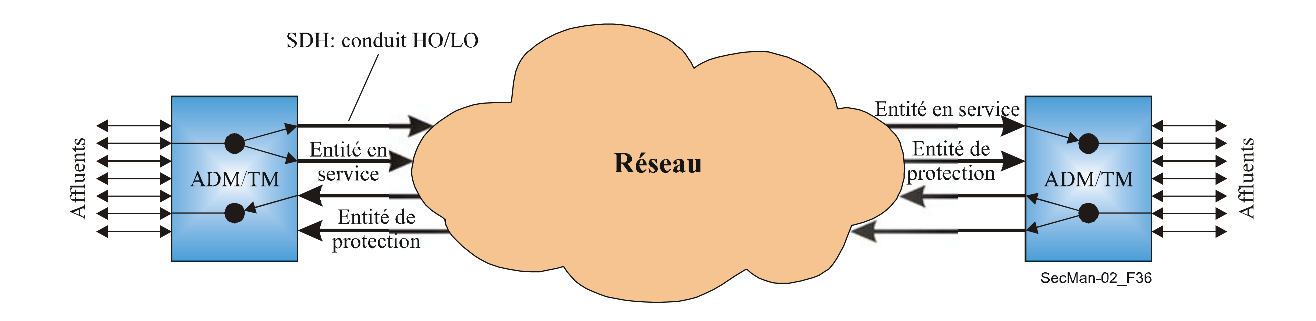


Figure 7-10 – Commutation de protection SNCP

La protection SNCP est fondée sur les conduits. Ainsi, un seul signal (AU-3, AU-4, etc.) est commuté à la fois. On peut aussi considérer cette protection comme une protection 1+1 unidirectionnelle pour les conduits individuels. La commutation de protection est réalisée au niveau des conduits:

- SDH: conteneur virtuel d'ordre supérieur HO – VC-4/3,
  unité d'affluent d'ordre inférieur LO – TU-3/2/11/12

Aucun protocole n'est utilisé (sauf pour la commutation forcée). La décision de commutation entre une entité en service et une entité de protection est fondée sur les conditions locales, lorsque les deux entités sont surveillées.

- Le temps nécessaire pour la commutation de protection doit être inférieur à 50 ms. Ainsi, si une fibre à haut débit, par exemple à 10 Gbit/s ou à 40 Gbit/s, est rompue et que tous les conduits font l'objet d'une protection SNCP, cet objectif de temps ne peut généralement pas être rempli si la commutation de protection est réalisée par des moyens logiciels, avec traitement des défauts dans un automate à états et échange de messages entre contrôleur de bord et contrôleur central.

7.4 Rétablissement

La Rec. UIT-T G.805 décrit des techniques d'amélioration de la disponibilité du réseau de transport. Elle emploie les termes "protection" (remplacement d'une ressource défaillante par un secours assigné au préalable) et "rétablissement" (remplacement d'une ressource défaillante avec un reroutage utilisant une capacité de rechange) pour le classement de ces techniques. Les actions de protection s'effectuent en général dans un délai de l'ordre de dizaines de millisecondes, alors que les actions de rétablissement prennent normalement un temps allant de centaines de millisecondes à plusieurs secondes.

Le plan de commande du réseau optique à commutation automatique (ASON, *automatic switched optical network*) permet à un opérateur de réseau d'offrir à l'utilisateur des appels avec une classe de service (CoS, *class of service*) sélectionnable (définissant, par exemple, la disponibilité, la durée des interruptions, les secondes avec erreur, etc.). Les mécanismes de protection et de rétablissement (utilisés par le réseau) permettent de prendre en charge la classe de service demandée par l'utilisateur. Le choix du mécanisme de survie (protection, rétablissement ou aucun) pour une connexion donnée prenant en charge un appel sera basé sur la politique de l'opérateur de réseau, la topologie du réseau et les capacités de l'équipement installé. Il est possible d'utiliser divers mécanismes de survie sur les connexions qui sont concaténées pour la fourniture d'un appel. Si un appel transite par les réseaux de plusieurs opérateurs, chacun de ces réseaux sera alors responsable de la survie des connexions de transit. Les demandes de connexion au niveau des interfaces UNI ou E-NNI contiendront uniquement la classe de service demandée et non un type explicite de protection ou de rétablissement.

La protection ou le rétablissement d'une connexion peut être invoqué ou désactivé de manière temporaire par une commande du plan de gestion. L'utilisation de ces commandes permet également d'effectuer des activités de maintenance programmées à l'avance et de se substituer au fonctionnement automatique dans certaines situations de défaillance exceptionnelles.

Voir la Rec. UIT-T G.8080/Y.1304.

7.5 Installations extérieures

La sécurité dans les systèmes de télécommunication recouvre de nombreux aspects. Les aspects liés à la sécurité physique des installations extérieures sont également étudiés par l'UIT-T. Il s'agit notamment de faire en sorte que les éléments matériels des systèmes résistent aux menaces d'incendie, de catastrophe naturelle et d'intrusion intentionnelle ou accidentelle de personnes. Les deux principaux points étudiés concernant la sécurité sont les suivants: faire en sorte que les composants des systèmes, câbles, enceintes, armoires, etc., puissent résister physiquement aux endommagements et surveiller les systèmes afin de prévenir autant que possible les endommagements ou de réagir aux problèmes et de rétablir la fonctionnalité des systèmes le plus rapidement possible.

D'une manière générale, les facteurs les plus importants à prendre en compte pour ces aspects de sécurité sont les suivants:

- cause de l'endommagement/de la perte de données:
  - maintenance de réseau;
  - accidents et calamités (non voulus);
  - vandalisme (voulu; aléatoire);
  - accès par du personnel non qualifié (par exemple personnes civiles, techniciens d'autres opérateurs);
  - criminalité (par exemple endommagement de terminal ou de brasseur dans un cambriolage; vol de câbles; écoute clandestine sur un câble); et
  - force ou violence concentrée voulue;
- situations environnementales des installations:
  - installations intérieures (centraux, locaux des abonnés);
  - installations extérieures aériennes (exposition à des faits humains/naturels);
  - installations extérieures au niveau de la rue (possibilité d'endommagements dus aux travaux); et
  - installations extérieures souterraines (dans des conduits ou directement enterrées).

D'une manière générale, on peut recommander que les précautions suivantes soient prises concernant la couche physique. La plupart de ces précautions sont gérées suivant les pratiques et règles locales des différents opérateurs:

- éviter d'utiliser des nœuds au niveau de la rue (armoires, socles, boîtes de jonction): compte tenu de la sensibilité aux accidents, au vandalisme, aux actes violents, aux incendies et à la curiosité générale, il est plus sûr d'utiliser des nœuds et des câbles souterrains;
- les armoires (ou autres coffrets) au niveau de la rue devraient être inviolables;
- toutes les enceintes devraient pouvoir être verrouillées ou scellées, afin d'éviter tout accès non souhaité;
- les câbles sont moins vulnérables en conduit que directement enterrés (par exemple, endommagements accidentels dus à des opérations de creusement);
- les points de terminaison ou de délimitation peuvent présenter une séparation (verrouillable) entre le côté réseau et le côté client, ou entre circuits utilisés par différents opérateurs;
- les terminaux des clients sont moins vulnérables à l'intérieur qu'à l'extérieur (montés sur un mur) (par exemple en cas de cambriolage);
- il peut être recommandé de conserver une longueur de câble supplémentaire en des emplacements réguliers dans le réseau, pour faciliter les réparations en cas d'endommagement accidentel (aussi bien pour les câbles aériens que pour les câbles souterrains);
- pour les installations à fibres optiques, il est recommandé de prévoir un niveau correct de séparation des circuits et une certaine stabilité optique dynamique, pour éviter toute perte de données/perturbation du trafic pendant la maintenance du réseau;
- pour les lignes vitales, il peut être recommandé de prévoir une redondance (lignes de secours) fondée sur des câbles et des réseaux séparés physiquement (par exemple structures en anneaux pour les banques, les hôpitaux).

D'autres mesures peuvent être implémentées, à savoir:

- établir des procédures de sécurité pour les installations extérieures;
- installer des systèmes de détection des incendies, de surveillance et de contrôle des installations extérieures;
- établir des critères afin d'évaluer si plusieurs opérateurs assurant des multiservices (POTS, RNIS, xDSL, etc.) peuvent coexister en toute sécurité dans la même partie du réseau sans aucune sorte d'interaction préjudiciable;
- utiliser des solutions techniques facilitant l'implémentation du dégroupage tout en maintenant l'intégrité, la fiabilité et l'interopérabilité dans les topologies de réseau couramment utilisées dans le monde entier;
- installer des dispositifs de signalisation le long des câbles souterrains;
- prévoir des systèmes de surveillance, d'aide à la maintenance et de test pour les installations extérieures;
- porter une attention particulière à la conception des câbles, dont le rôle principal est de protéger l'intégrité physique du support de transmission – les fibres optiques; et
- tenir compte des aspects liés à la construction des câbles, à l'épissurage des fibres, aux platines d'assemblage et aux enceintes, aux unités de branchement, à la planification des itinéraires, aux caractéristiques des navires câbliers, aux activités de chargement et de pose, aux méthodes de réparation, aux protections et aux méthodes de test applicables aux câbles à fibres optiques de terre marinisés.

8 Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication

La gestion et la connaissance de la sécurité comportent un certain nombre de processus, notamment la définition de structures et de procédures pour le traitement et la diffusion d'informations sur les incidents relatifs à la sécurité. Des experts de l'UIT-T ont réagi à un besoin exprimé dans ce domaine et ont élaboré la Rec. UIT-T E.409. Cette Recommandation, intitulée *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication*, a pour objet d'analyser, de structurer et de proposer une méthode permettant d'organiser la prise en charge des incidents au sein d'une organisation de télécommunication participant à la fourniture de télécommunications internationales, en fonction du déroulement et de la nature des incidents. Le déroulement des incidents et leur prise en charge interviennent lorsqu'il s'agit de classer un événement comme un simple événement, comme un incident, comme une atteinte à la sécurité ou comme une situation de crise. Le déroulement des incidents joue aussi un rôle dans les premières décisions importantes qui doivent être prises.

Cette Recommandation donne un aperçu général et des orientations en ce qui concerne la préparation de l'organisation en cas d'incident et de la prise en charge des atteintes à la sécurité.

Elle est générique par nature et n'énonce ni n'aborde des exigences destinées à des réseaux particuliers.

Cette Recommandation vise à faciliter l'amélioration à l'échelle internationale de la sécurité des réseaux de télécommunication, mais cette amélioration pourrait être facilitée si les exigences énoncées dans cette Recommandation pouvaient également être appliquées aux réseaux d'information et de communication (ICN, *information and communication network*) nationaux.

L'emploi fortement accru de l'ordinateur dans le domaine des télécommunications internationales entraîne dans son sillage la criminalité informatique. Au cours des dernières années, cette criminalité a littéralement explosé, ainsi que l'ont démontré plusieurs enquêtes menées aux niveaux international et national. Dans la plupart des pays, on ne connaît pas le nombre exact d'intrusions informatiques, ni d'incidents, en particulier ceux qui sont liés aux télécommunications internationales.

La majorité des organisations ou des sociétés de télécommunication ne sont pas spécialement organisées pour gérer les atteintes à la sécurité des réseaux ICN, bien qu'elles puissent disposer d'équipes polyvalentes chargées de gérer les différents types de crises. Lorsqu'un incident relatif à la sécurité d'un réseau ICN se produit, il est traité ponctuellement, c'est-à-dire la personne qui le détecte prend la responsabilité de le traiter au mieux. Dans certaines organisations, on a tendance à oublier et à dissimuler les atteintes à la sécurité des réseaux ICN, parce qu'elles sont susceptibles d'affecter la production, la disponibilité et les recettes.

Souvent, lorsqu'une atteinte à la sécurité d'un réseau ICN est détectée, la personne qui la détecte ne sait pas qui elle devrait aviser. Dans le secteur informatique, il se peut alors que l'administrateur du système ou du réseau se borne, pour se débarrasser du problème, à trouver une solution de rechange ou un bricolage hâtif. Il ne dispose ni des pouvoirs, ni du temps, ni de l'expérience nécessaires pour apporter des corrections au système afin que l'incident touchant à la sécurité du réseau ICN ne se reproduise plus. Pour ces raisons majeures, il vaut mieux disposer d'une unité ou d'un groupe formé qui puisse prendre en charge promptement et correctement les atteintes à la sécurité. De nombreuses questions peuvent en outre concerner des domaines aussi divers que celui des relations avec les médias, le domaine juridique, le domaine relatif à l'application des lois, celui de la part de marché ou le domaine financier.

L'emploi de classifications différentes, lors de la notification ou de la prise en charge d'un incident, peut conduire à des malentendus qui peuvent par la suite empêcher qu'une atteinte à la sécurité d'un réseau ICN reçoive l'attention convenable ou la prise en charge rapide qui seraient nécessaires pour y mettre fin, pour la contenir et pour l'empêcher de se reproduire. Cela peut avoir de sérieuses conséquences sur l'organisation touchée (la victime).

Pour maîtriser la prise en charge des incidents et leur notification, il convient de comprendre comment ils sont détectés, pris en charge et résolus. L'établissement d'une structure générale de traitement des incidents (à savoir, les incidents physiques, administratifs ou organisationnels, et logiques) permet d'obtenir une image générale de la nature et du déroulement d'un incident. Une terminologie uniformisée assure une compréhension commune des mots et des termes.

8.1 Définitions

L'"atteinte à la sécurité" est définie comme étant "une infraction à la sécurité, une menace à l'égard de celle-ci, une faiblesse et un dysfonctionnement qui pourraient avoir une incidence sur la sécurité des biens institutionnels". Dans cette Recommandation, on suppose qu'un incident est moins grave qu'une atteinte à la sécurité et qu'une atteinte à la sécurité informatique est un type particulier d'atteinte à la sécurité.

La Figure 8-1 illustre la pyramide des événements. A la base est situé l'événement, suivi de l'incident, de l'atteinte à la sécurité, et au sommet sont situées la crise et la catastrophe. Plus un événement est proche du sommet, plus il est grave. Afin qu'il soit fait usage d'un vocabulaire commun et pertinent en ce qui concerne la prise en charge des incidents dans les réseaux ICN, il est recommandé d'utiliser les définitions suivantes:

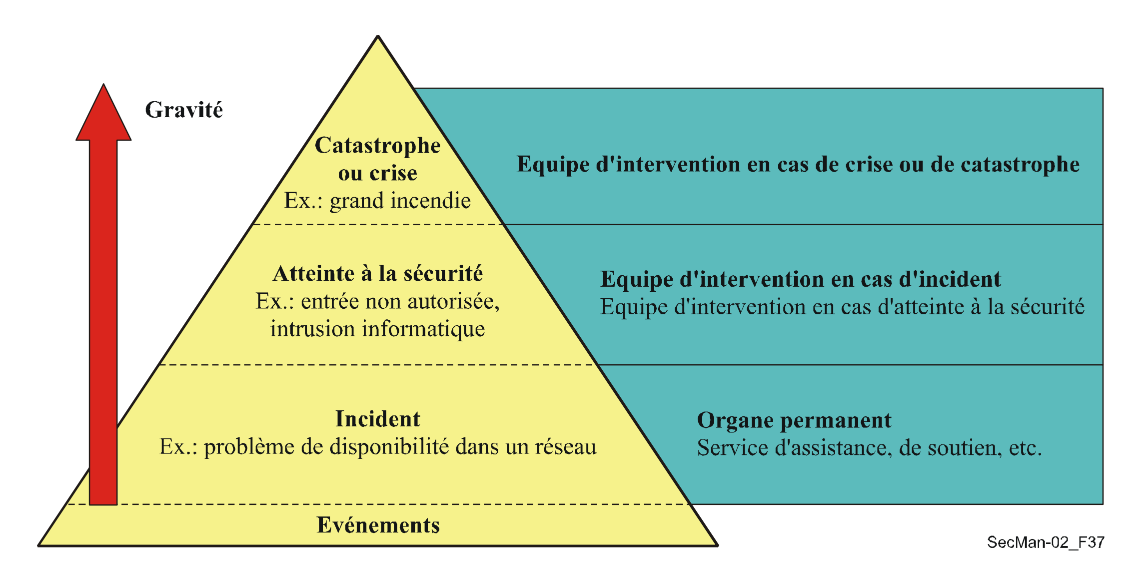


Figure 8-1 – Pyramide des événements (Rec. UIT-T E.409)

8.1.1 événement: fait observable, qu'il n'est pas possible de prédire ou de contrôler (complètement).

8.1.2 incident: événement pouvant conduire à un fait ou à un épisode peu grave.

8.1.3 atteinte à la sécurité: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

8.1.4 atteinte à la sécurité des réseaux d'information et de communication (ICN): tout événement concret ou soupçonné d'être préjudiciable, en rapport avec la sécurité des réseaux ICN. On peut indiquer à titre d'exemple:

- l'intrusion par le réseau dans les systèmes informatiques des réseaux ICN;
- la présence de virus informatiques;
- le sondage par le réseau de la vulnérabilité d'une gamme de systèmes informatiques;
- la perte d'appels au niveau des autocommutateurs privés;
- tout autre événement non désiré résultant d'actions non autorisées, intérieures ou extérieures (attaques par déni de service, catastrophes et autres situations d'urgence, etc.).

8.1.5 crise: état résultant d'un événement ou de la connaissance d'un événement à venir qui pourrait avoir de graves conséquences néfastes. Au cours d'une crise, on peut, dans le meilleur des cas, avoir la possibilité de prendre des mesures pour éviter que cette crise ne devienne une catastrophe. Lorsqu'une *catastrophe* se produit, on dispose généralement d'un plan d'urgence pour les entreprises (BCP, *business continuency plan*) et d'une équipe de gestion de la crise pour prendre en charge la situation.

8.2 Démarche logique

Il est recommandé que les organisations de télécommunication créant, en une première étape, des équipes d'intervention en cas d'incident (relatif à la sécurité informatique), fassent savoir, pour éviter des malentendus, qu'elles emploient une classification. La collaboration est beaucoup plus facile si l'on emploie le même "langage".

Il est aussi recommandé que les organisations utilisent les termes "incident" et "atteinte à la sécurité des réseaux ICN", et définissent leurs subdivisions en fonction de la gravité de ceux-ci. Par nature, une atteinte à la sécurité d'un réseau ICN est un événement non désiré ou non autorisé. Cela veut dire que les atteintes à la sécurité des réseaux ICN englobent les intrusions informatiques, les attaques par déni de service ou les virus, en fonction de la motivation, de l'expérience et des ressources documentées disponibles dans l'entreprise. Dans les organisations qui disposent de vraies équipes destinées à combattre les virus, ceux-ci peuvent ne pas être considérés comme des atteintes à la sécurité des réseaux ICN, mais seulement comme des incidents.

Un exemple ou modèle d'une telle subdivision est le suivant:

– Incidents
  - violation de l'éthique en vigueur sur Internet (pollupostage, contenu abusif, etc.);
  - violation des politiques en matière de sécurité;
  - virus isolés.
– Atteintes à la sécurité des réseaux ICN
  - explorations et sondages;
  - intrusions informatiques;
  - sabotage et endommagement informatiques (attaques bloquant l'accessibilité telles que le bombardement, attaques par déni de service);
  - logiciels malveillants (virus, cheval de Troie, vers, etc.);
  - vol d'informations et espionnage;
  - usurpation d'identité.

En employant la même granularité et la même précision dans la terminologie, il est possible d'acquérir de l'expérience en ce qui concerne les sujets suivants:

- indication relative à la gravité et à l'étendue;
- indication quant à la nécessité d'être rapide (par exemple pour rétablir le niveau de sécurité voulu);
- efforts en ce qui concerne les contre-mesures;
- coûts éventuels impliqués.

9 Conclusions

L'UIT-T a commencé il y a longtemps à élaborer un ensemble de Recommandations fondamentales sur la sécurité: X.800 est un document de référence sur l'architecture de sécurité pour l'interconnexion des systèmes ouverts et la série X.810-X.816 définit un cadre de sécurité pour les systèmes ouverts, les Recommandations de cette série traitant respectivement de l'aperçu général, de l'authentification, du contrôle d'accès, de la non-répudiation, de la confidentialité, de l'intégrité et enfin de l'audit et des alarmes de sécurité. Plus récemment, la Rec. UIT-T X.805 a été élaborée en vue de décrire l'architecture de sécurité pour les systèmes assurant des communications de bout en bout. La modification architecturale que la Rec. UIT-T X.805 représente tient compte des menaces et vulnérabilités plus nombreuses qui résultent d'un environnement devenu multiréseaux et multifournisseurs de services. La Rec. UIT-T X.509 portant sur le cadre général des certificats de clé publique et d'attribut est certainement le texte de l'UIT-T auquel il est le plus souvent fait référence en matière d'applications de sécurité, soit directement, soit implicitement dans d'autres normes reposant sur les principes énoncés dans la Rec. UIT-T X.509.

En plus de ces Recommandations cadres, l'UIT-T a établi des dispositions relatives à la sécurité de plusieurs systèmes et services définis dans ses Recommandations. Le paragraphe 6 du présent manuel décrit notamment les applications suivantes: téléphonie IP utilisant H.323 ou IPCablecom, transmission sécurisée de télécopie et gestion de réseau. Il donne également un exemple d'application des infrastructures de clé publique et de gestion de privilège à la télésanté. Il convient de noter qu'il existe de nombreux *autres* domaines dans lesquels les besoins de sécurité sur le plan des télécommunications et des technologies de l'information sont pris en considération dans les Recommandations de l'UIT-T. Ces domaines et des aspects tels que la prévention des fraudes et le retour à la normale après une catastrophe, examinés au sein de plusieurs Commissions d'études de l'UIT-T, seront abordés plus en détail dans de futures éditions. A l'appui de ses travaux sur la sécurité, l'UIT-T organise ou participe à des séminaires ou ateliers internationaux sur la sécurité, développe un projet de sécurité, a désigné une commission d'études directrice pour les travaux de l'UIT-T sur la sécurité et collabore avec d'autres organisations de normalisation (par exemple ISO/CEI JTC 1/SC 27).

Références

En plus des Recommandations de l'UIT-T (qui figurent à l'adresse http://www.itu.int/ITU-T/publications/recs.html) mentionnées dans le présent manuel, les documents suivants ont également été utilisés.

[ApplCryp] SCHNEIER (B.), *"Applied Cryptography – Protocols, Algorithms and Source Code in C"* (Cryptographie appliquée – protocoles, algorithmes et code source en C) 2e édition, Wiley, 1996; ISBN 0-471-12845-7

[Chadwick] CHADWICK (D.W.), *"The Use of X.509 in E-Healthcare"* (Utilisation de la Recommandation X.509 dans le domaine de la télésanté), atelier sur la normalisation dans le domaine de la télésanté; Genève, 23-25 mai 2003; fichier PowerPoint à l'adresse www.itu.int/itudoc/itu-t/workshop/e-health/s5-02.html et présentation audio à l'adresse www.itu.int/ibs/ITU-T/e-health/Links/B-20030524-1100.ram

[Euchner] EUCHNER (M.), PROBST (P.-A.), *"Multimedia Security within Study Group 16: Past, Present and Future"* (Sécurité des systèmes multimédias au sein de la Commission d'études 16: passé, présent et avenir), atelier de l'UIT-T sur la sécurité; 13-14 mai 2002, Séoul, Corée; www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html

[FreePresc] Statistiques relatives à la gratuité des médicaments au Royaume-Uni; www.doh.gov.uk/public/sb0119.htm

[Packetizer] *"A Primer on the H.323 Series Standard"* (Eléments fondamentaux concernant la norme H.323)
www.packetizer.com/iptel/h323/papers/primer/

[Policy] CHADWICK (D.W.), MUNDY (D.), *"Policy Based Electronic Transmission of Prescriptions"* (Transmission électronique des ordonnances fondée sur des politiques); IEEE POLICY 2003, 4-6 juin, lac de Côme, Italie.
sec.isi.salford.ac.uk/download/PolicyBasedETP.pdf

[CE 17] Commission d'études 17 de l'UIT-T; "Commission d'études directrice pour la sécurité des télécommunications"
www.itu.int/ITU-T/studygroups/com17/tel-security.html
(catalogue des Recommandations approuvées relatives à la sécurité des télécommunications; définitions relatives à la sécurité approuvées par l'UIT-T)

[Shannon] SHANNON (G.); *"Security Vulnerabilities in Protocols"* (Vulnérabilités de sécurité dans les protocoles); atelier de l'UIT-T sur la sécurité; 13-14 mai 2002, Séoul, Corée; www.itu.int/itudoc/itu-t/workshop/security/present/s1p2.html

[Wisekey] MANDIL (S.), DARBELLAY (J.), *"Public Key Infrastructures in e-health"* (Infrastructures de clé publique dans le domaine de la télésanté); contribution écrite à l'atelier sur la normalisation dans le domaine de la télésanté; Genève, 23-25 mai 2003; www.itu.int/itudoc/itu-t/workshop/e-health/wcon/s5con002_ww9.doc

ISO/CEI 18033-1:2005, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 1: Généralités*

ISO/CEI 18033-2:2006, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 2: Chiffres asymétriques*

ISO/CEI 18033-3:2005, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 3: Chiffrement par blocs*

ISO/CEI 18033-4:2005, *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 4: Chiffrements en flot*

Annexe A
Catalogue des Recommandations de l'UIT-T relatives à la sécurité

Etabli par la Commission d'études 17 de l'UIT-T, Commission d'études directrice pour la sécurité des télécommunications

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
E.408	Prescriptions de sécurité des réseaux de télécommunication	Cette Recommandation donne un aperçu général des prescriptions de sécurité et définit un cadre qui identifie les menaces qui pèsent sur la sécurité des réseaux de télécommunication en général (fixes ou mobiles; voix et données) et indique comment planifier des contre-mesures afin de limiter les risques découlant de ces menaces.	CE 2
E.409	Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication	Cette Recommandation a pour objet d'analyser, de structurer et de proposer une méthode permettant d'organiser la prise en charge des incidents au sein d'une organisation de télécommunication participant à la fourniture de télécommunications internationales, en fonction du déroulement et de la nature des incidents. Le déroulement des incidents et leur prise en charge interviennent lorsqu'il s'agit de classer un événement comme un simple événement, comme un incident, comme une atteinte à la sécurité ou comme une situation de crise. Le déroulement des incidents joue aussi un rôle dans les premières décisions importantes qui doivent être prises. Pour maîtriser la prise en charge des incidents et leur notification, il convient de comprendre comment ils sont détectés, pris en charge et résolus. L'établissement d'une structure générale de traitement des incidents (à savoir, les incidents physiques, administratifs ou organisationnels, et logiques) permet d'obtenir une image générale de la nature et du déroulement d'un incident. Une terminologie uniformisée assure une compréhension commune des mots et des termes.	CE 17
F.400	Aperçu général du système et du service de messagerie	Cette Recommandation donne un aperçu permettant de définir globalement le système et le service d'un MHS et sert d'aperçu général du MHS. Cet aperçu s'insère dans un ensemble de Recommandations qui décrivent le modèle et les éléments de service du système et des services de messagerie (MHS). Cette Recommandation offre un aperçu des capacités d'un MHS qui sont utilisées par le fournisseur du service pour la fourniture de services de messagerie (MH, *message handling*) publics permettant aux utilisateurs d'échanger des messages selon le principe de l'enregistrement et de la retransmission. Le système de messagerie est conçu conformément aux principes du modèle de référence de l'interconnexion des systèmes ouverts (modèle de référence OSI) pour les applications de l'UIT-T (Rec. UIT-T X.200) et il utilise les services de la couche Présentation et les services fournis par d'autres éléments plus généraux du service d'application. Un MHS peut être constitué au moyen de tout réseau entrant dans le cadre OSI. Le service de transfert de messages assuré par le MTS est indépendant de l'application. Le service IPM (F.420 + X.420), le service de messagerie EDI (F.435 + X.435) et le service de messagerie vocale (F.440 + X.440) constituent des exemples d'application normalisée. Les systèmes d'extrémité peuvent utiliser le service de transfert de messages (MT, *message transfer*) pour des applications particulières définies par accord bilatéral. Les services de messagerie assurés par le fournisseur du service font partie du groupe de services télématiques. Les services publics construits sur le MHS ainsi que l'accès au MHS ou depuis le MHS pour les services publics sont définis dans les Recommandations de la série F.400. Les aspects techniques du MHS sont définis dans les Recommandations de la série X.400. L'architecture globale du système de messagerie est définie dans la Rec. UIT-T X.402. Les éléments de service sont les caractéristiques de service fournies par les processus d'application. Les éléments de service sont considérés comme étant des composantes des services offerts aux utilisateurs et sont soit des éléments d'un service de base, ou des fonctionnalités optionnelles d'utilisateur, ces dernières étant classées en fonctionnalités principales d'utilisateur et en fonctionnalités additionnelles d'utilisateur. Les capacités de sécurité du MHS sont décrites au § 15/F.400, y compris les menaces de sécurité du MHS, le modèle de sécurité, les éléments de service décrivant les fonctionnalités de sécurité (définis dans l'Annexe B), la gestion de la sécurité, les effets liés à la sécurité du MHS, la sécurité du service IPM.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
F.440	Services de messagerie: le service de messagerie vocale	Cette Recommandation décrit les caractéristiques générales d'exploitation et de qualité de service du service public international de messagerie vocale (VM, *voice messaging*), un type particulier de service de messagerie (MH) (*message handling*), qui est un service de télécommunication international offert par les Administrations et qui permet aux abonnés d'envoyer un message à un ou plusieurs destinataires et de recevoir des messages au moyen de réseaux de télécommunication utilisant conjointement des techniques d'enregistrement et de retransmission et des techniques d'enregistrement et interrogation. Le service de messagerie vocale permet aux abonnés de demander l'exécution de diverses fonctions pendant le traitement et l'échange de messages vocaux codés. Certaines fonctions sont propres au service de messagerie vocale de base. D'autres fonctions, qui ne sont pas des fonctions de base, peuvent, si elles sont fournies par les Administrations, être sélectionnées par l'usager pour chaque message ou pour une période convenue aux termes d'un contrat. L'intercommunication avec le service de messagerie de personne à personne (IPM, *interpersonal messaging*) peut être assurée en option dans le service de messagerie vocale. Il appartient aux Administrations de fournir les fonctions de base au niveau international. Les fonctions autres que les fonctions de base, visibles pour l'abonné, sont classées en fonctions essentielles et fonctions supplémentaires. Les Administrations sont tenues de fournir les fonctions facultatives essentielles au niveau international. Certaines Administrations peuvent fournir des fonctions facultatives supplémentaires pour un usage national et sur le plan international sur la base d'accords bilatéraux. Les fonctions autres que les fonctions de base sont appelées fonctions facultatives d'usager. Il est possible d'assurer le service de messagerie vocale en empruntant un réseau de communication quelconque. Ce service peut être offert séparément ou en association avec divers services télématiques ou de transmission de données. Les spécifications techniques et les protocoles à utiliser dans le service de messagerie vocale sont définis dans les Recommandations de la série X.400. Annexe G: Eléments de service de sécurité en messagerie vocale; Annexe H: Aperçu de la sécurité en messagerie vocale.	CE 17
F.851	Télécommunications personnelles universelles – Description du service (ensemble de services 1)	Cette Recommandation a pour but de fournir la description du service des télécommunications personnelles universelles (UPT, *universal personnal telecommunication*) et de proposer des dispositions concernant son exploitation. Elle contient une description générale du service du point de vue de l'utilisateur ou abonné individuel des UPT. Ainsi, l'utilisateur UPT participe à un ensemble personnalisé de services souscrits par abonnement, à partir desquels il définit ses besoins personnels pour former le profil du service UPT. L'utilisateur UPT peut utiliser le service UPT avec un risque minimum de violation du secret ou de taxation erronée due à une utilisation frauduleuse. En principe, tout service de télécommunication de base peut être utilisé avec le service UPT. Les services fournis à l'utilisateur UPT sont limités uniquement par les réseaux et les terminaux utilisés. "*L'authentification de l'identité* de l'utilisateur UPT" est la première des fonctions essentielles d'utilisateur et l'*authentification du fournisseur* de service UPT constitue une fonctionnalité facultative d'utilisateur. Le § 4.4 traite des prescriptions de sécurité.	CE 2
G.808.1	Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux	Cette Recommandation donne un aperçu de la commutation de protection linéaire. Elle porte sur les systèmes de protection fondés sur les réseaux de transport optiques (OTN, *optical transport network*), sur les réseaux utilisant la hiérarchie numérique synchrone (SDH, *synchronous digital hierarchy*) et sur les réseaux utilisant le mode de transfert asynchrone (ATM, *asynchronous transfer mode*). L'aperçu des schémas de protection en anneau et de protection de sous-réseaux interconnectés (anneau par exemple) fera l'objet d'autres Recommandations.	CE 15
G.827	Paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant	Cette Recommandation définit les paramètres et objectifs de performance du réseau pour les éléments de conduit et la disponibilité de bout en bout des conduits numériques internationaux à débit constant. Ces paramètres sont indépendants du type de réseau physique prenant en charge le conduit de bout en bout (réseau à fibres optiques, hertzien ou à satellite, par exemple). D'autre part, cette Recommandation donne des précisions sur les méthodes permettant d'améliorer la disponibilité et de calculer la disponibilité de bout en bout d'un ensemble d'éléments de réseau.	CE 12

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
G.841	Types et caractéristiques des architectures de protection des réseaux à hiérarchie numérique synchrone	Cette Recommandation décrit les divers mécanismes de protection pour des réseaux en hiérarchie numérique synchrone (SDH) ainsi que leurs objectifs et leurs applications. Les mécanismes de protection sont classés comme suit: protection d'un chemin SDH (au niveau de la section ou de la couche conduit) et protection d'une connexion de sous-réseau SDH (avec supervision intrinsèque, supervision sans intrusion et supervision de sous-couche).	CE 15
G.842	Interfonctionnement des architectures de protection des réseaux à hiérarchie numérique synchrone	Cette Recommandation décrit les mécanismes d'interfonctionnement entre architectures de protection de réseau. L'interfonctionnement décrit ici s'applique à l'interconnexion à un nœud et à deux nœuds pour l'échange de trafic entre anneaux. Chaque anneau peut être configuré pour la protection partagée de section(s) de multiplexage ou pour la protection SNCP.	CE 15
G.873.1	Réseau de transport optique: protection linéaire	Cette Recommandation définit le protocole de commutation de protection automatique (APS, *automatic protection switching*) et l'opération de commutation de protection pour les systèmes de protection linéaire du réseau de transport optique au niveau des unités de données de canal optique (ODUk, *optical channel data unit*). Les systèmes de protection examinés dans cette Recommandation sont les suivants: protection de chemin par unité ODUk; protection de connexion de sous-réseau par unité ODUk avec surveillance intrinsèque; protection de connexion de sous-réseau par unité ODUk avec surveillance non intrusive; protection de connexion de sous-réseau par unité ODUk avec surveillance de sous-couche.	CE 15
G.911	Paramètres et méthodes de calcul de la fiabilité et de la disponibilité des systèmes à fibres optiques	Cette Recommandation définit un ensemble minimal de paramètres nécessaires pour décrire la fiabilité et la disponibilité des systèmes à fibres optiques, à savoir la fiabilité et la maintenance des systèmes, la fiabilité des dispositifs optiques actifs, la fiabilité des dispositifs optiques passifs ainsi que la fiabilité des fibres et câbles optiques. Cette Recommandation définit en outre des lignes directrices et des méthodes, accompagnées d'exemples, pour calculer la fiabilité prévue des dispositifs, ensembles et systèmes.	CE 15
H.233	Système de confidentialité pour les services audiovisuels	Un système de protection des données privées comprend deux parties, le *mécanisme de confidentialité* ou *processus de chiffrement* des données et un sous-système de *gestion de clés*. Cette Recommandation décrit la partie mécanisme de confidentialité d'un système de protection des données privées destiné à être utilisé dans les services audiovisuels à bande étroite. Bien qu'un tel système de protection des données privées nécessite un *algorithme de chiffrement*, la spécification de cet algorithme n'est pas incluse ici: le système admet plusieurs algorithmes spécifiques. Le *système de confidentialité* est applicable aux liaisons point à point entre terminaux ou entre un terminal et un pont de conférence (MCU, *multipoint control unit*); son application peut être élargie au fonctionnement multipoint sans chiffrement dans le pont de conférence	CE 16
H.234	Gestion des clés de chiffrement et système d'authentification pour les services audiovisuels	Un *système de chiffrement* comprend deux parties, le *mécanisme de confidentialité* ou *processus de chiffrement* des données, et un sous-système de *gestion de clés*. Cette Recommandation décrit les méthodes d'*authentification* et de *gestion des clés* pour un système de chiffrement destiné à être utilisé dans les services audiovisuels à bande étroite. La *confidentialité* est assurée à l'aide de *clés secrètes*. Ces clés sont chargées dans le *mécanisme de chiffrement* du système de confidentialité et régissent la manière dont les données transmises sont chiffrées et déchiffrées. Si un tiers accède aux clés utilisées, le système de chiffrement n'est plus sûr. La maintenance des clés par les utilisateurs est donc un élément important de tout système de confidentialité. Trois méthodes pratiques de *gestion des clés* sont spécifiées dans cette Recommandation.	CE 16

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
H.235	Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)	Cette Recommandation décrit des améliorations apportées dans le cadre de la série des Recommandations H.3xx afin d'y introduire des *services de sécurité* tels que l'*authentification* et le *secret des communications* (*chiffrement des données*). Le procédé qui est proposé est applicable aussi bien aux simples conférences point à point qu'aux conférences point à multipoint, à partir de tous les terminaux faisant appel au protocole de commande décrit dans la Rec. UIT-T H.245. Par exemple, les systèmes H.323 fonctionnent sur des réseaux en mode paquet qui n'offrent pas une qualité de service garantie. La *sûreté* et la qualité *du service* offert par le réseau de base sont absentes pour les mêmes raisons techniques. Des communications sûres et en temps réel sur des réseaux non sûrs soulèvent généralement deux grands types de préoccupation: l'*authentification* et le *secret des communications*. Cette Recommandation décrit l'infrastructure de sécurité et les *techniques* spécifiques de *secret des communications* que les terminaux multimédias conformes à la série H.3xx doivent utiliser. Elle traite les questions relatives aux conférences interactives, c'est-à-dire, entre autres domaines, *l'authentification et le secret des communications* de tous les flux médias échangés en temps réel au cours d'une conférence. Elle indique le protocole et les algorithmes nécessaires entre les entités H.323. Elle fait appel aux capacités générales qui sont décrites dans la Rec. UIT-T H.245: toute norme d'exploitation liée à ce protocole de commande pourra donc utiliser ce cadre de sécurité. L'on prévoit que, dans la mesure du possible, d'autres terminaux selon la série H pourront interfonctionner et utiliser directement les méthodes décrites dans cette Recommandation. Dans un premier temps, cette Recommandation n'assurera pas une implémentation complète dans tous les domaines. Elle développera spécifiquement l'*authentification des points d'extrémité et le secret des communications multimédias*. Cette Recommandation prévoit la possibilité de négocier les services et les capacités de façon générique. Elle prévoit également la possibilité de sélectionner les techniques et capacités cryptographiques utilisées. Leur mode d'emploi particulier dépend des capacités des systèmes, des exigences d'application et des contraintes propres aux politiques de sécurité. Cette Recommandation prend en compte divers *algorithmes cryptographiques*, avec diverses options appropriées à différents objectifs, comme les longueurs des clés. Certains *algorithmes cryptographiques* peuvent être attribués à des services de sécurité spécifiques (par exemple un algorithme pour un chiffrement rapide du flux média et un autre pour le chiffrement de la signalisation). Il convient également de noter que certains des algorithmes ou mécanismes cryptographiques dont on dispose pourront être réservés à l'exportation ou à d'autres fins nationales (par exemple avec des clés de longueur restreinte). Cette Recommandation prend en compte la signalisation d'algorithmes notoires, en plus de celle d'algorithmes cryptographiques non normalisés ou privatifs. Aucun algorithme n'est spécifiquement prescrit mais il est fortement conseillé que les points d'extrémité prennent en charge autant d'algorithmes applicables que possible afin de réaliser l'interopérabilité. Ce conseil est à rapprocher de l'idée que la conformité à la Rec. UIT-T H.245 ne garantit pas l'interopérabilité de deux codecs d'entité. La version 2 de la Rec. UIT-T H.235, qui remplace la première, contient de nombreuses améliorations telles que la cryptographie à courbe elliptique, des profils de sécurité (de type à simple mot de passe ou à signature numérique perfectionnée), de nouvelles contre-mesures de sécurité (protection contre le spam de média), la prise en charge de l'algorithme de chiffrement avancé (AES, *advanced encryption algorithm*) et du service d'extrémité; elle définit des identificateurs d'objet et introduit des modifications tirées du guide à l'usage des responsables de l'implémentation de la Rec. UIT-T H.323. La version 3 de la Rec. UIT-T H.235, qui remplace la deuxième, définit une procédure applicable aux signaux DTMF chiffrés, des identificateurs d'objet pour l'algorithme de chiffrement AES des charges utiles de médias, le mode de chiffrement amélioré OFB des flux (mode EOFB) pour le chiffrement des flux de médias; elle décrit également une option d'authentification seulement dans l'Annexe D applicable au franchissement des dispositifs NAT/pare-feu, une procédure de distribution des clés sur le canal RAS, des procédures de transport de clé de session mieux sécurisé et des procédures de distribution et de mise à jour de clés de session plus fiables, des procédures permettant de sécuriser des flux de charge utile multiples, une meilleure prise en charge de la sécurité pour les appels acheminés directement (nouvelle Annexe I), des moyens plus souples de signalement des erreurs, des précisions et des améliorations d'efficacité pour la sécurité du démarrage rapide et pour la signalisation Diffie-Hellman avec des paramètres Diffie-Hellman plus longs et introduit des modifications tirées du guide à l'usage des responsables de l'implémentation de la Rec. UIT-T H.323.	CE 16

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
		Annexe F/H.235 *Profil de sécurité hybride*. Cette annexe décrit un *profil de sécurité hybride à base d'infrastructure de clés publiques* (PKI, *public key infrastructure*), efficace et modulable, utilisant les *signatures numériques* de l'Annexe E/H.235 et le *profil de sécurité élémentaire* de l'Annexe D/H.235. Cette annexe est proposée à titre d'option. Les *entités de sécurité* H.323 (terminaux, portiers, passerelles, ponts MCU, etc.) peuvent implémenter ce *profil de sécurité hybride* pour améliorer la sécurité ou pour l'assurer en cas de nécessité. Dans ce contexte, "hybride" signifie que les procédures de sécurité des profils de signature de l'Annexe E/H.235 sont en fait appliquées avec une certaine souplesse et que les signatures numériques restent conformes aux procédures RSA. Les *signatures numériques* ne sont cependant utilisées qu'en cas de nécessité absolue; en conditions normales, ce sont les *techniques de sécurité symétriques* hautement efficaces du profil de sécurité élémentaire de l'Annexe D/H.235 qui seront employées. Ce profil de sécurité hybride est applicable à la téléphonie IP "mondiale" modulable; il n'est pas exposé aux limitations du profil de sécurité élémentaire simple de l'Annexe D/H.235, lorsqu'il est appliqué de manière stricte. De plus, il n'est pas exposé à certains inconvénients du profil de l'Annexe E/H.235 tels qu'un plus grand besoin de largeur de bande et de performance lorsqu'il est appliqué de manière stricte. Par exemple, le profil de sécurité hybride ne dépend pas de l'administration (statique) de secrets mutuellement partagés dans les bonds de différents domaines. Les utilisateurs peuvent donc très facilement choisir leur fournisseur de téléphonie IP. Le profil de sécurité accepte une certaine mobilité de l'utilisateur. Par ailleurs, il n'applique la cryptographie asymétrique avec signatures et certificats qu'en cas de nécessité, se limitant sinon aux techniques symétriques, plus simples et plus efficaces. Il assure la tunnellisation des messages H.245 pour l'intégrité de ceux-ci. Il offre également des dispositions pour la non-répudiation des messages. Ce profil de sécurité hybride utilise le modèle acheminé par portier; il est fondé sur les techniques de tunnellisation H.245. La prise en charge de modèles non acheminés par portier nécessite un complément d'étude. Annexe G/H.235: *Utilisation du protocole de gestion de clés MIKEY en association avec le protocole de transport en temps réel sécurisé (SRTP) dans les systèmes H.235*. Cette Annexe permet de mettre en œuvre une sécurité de média SRTP IETF pour laquelle la gestion de clés MIKEY fournit les clés et les paramètres de sécurité nécessaires aux points d'extrémité concernés de bout en bout. L'Annexe G peut être mise en œuvre dans un domaine H.323 parmi des systèmes H.323 conformes à l'Annexe G/H.235. Elle définit les extensions en termes de protocole de sécurité relatives aux messages RAS et à la signalisation d'appel H.225.0 ainsi qu'au protocole H.245 et définit aussi les procédures correspondantes. Elle spécifie en outre les capacités permettant de prendre en charge l'interfonctionnement avec les entités SIP IETF qui ont implémenté la gestion de clés MIKEY et le protocole SRTP. Il convient de noter que cette annexe est écrite sous la forme d'un profil de sécurité H.235 qui est offert en option et qui peut compléter les autres fonctionnalités de sécurité de média H.235 (Annexe B, Annexe D.7). NOTE – La Rec. UIT-T H.235 a été restructurée comme suit: • H.235.0, Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245) • H.235.1, Cadre de sécurité H.323: profil de sécurité de base • H.235.2, Cadre de sécurité H.323: profil de sécurité avec signature • H.235.3, Cadre de sécurité H.323: profil de sécurité hybride • H.235.4, Cadre de sécurité H.323: sécurité des appels à routage direct et des appels à routage sélectif • H.235.5, Cadre de sécurité H.323: cadre de l'authentification sécurisée pendant l'échange de messages RAS au moyen de secrets partagés faibles • H.235.6, Cadre de sécurité H.323: profil pour le chiffrement vocal avec gestion de clés native dans les systèmes H.235/H.245 • H.235.7, Cadre de sécurité H.323: utilisation du protocole de gestion de clés MIKEY avec le protocole de transport en temps réel sécurisé (SRTP) dans les systèmes H.235 • H.235.8, Cadre de sécurité H.323: échange de clés dans le protocole SRTP au moyen de canaux de signalisation sécurisés • H.235.9, Cadre de sécurité H.323: prise en charge des passerelles de sécurité dans les systèmes H.323	

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
H.323	Systèmes de communication multimédia en mode paquet	Cette Recommandation décrit les terminaux et autres entités qui assurent des services en temps réel de communications audio, vidéo, de données et/ou multimédias sur des réseaux en mode paquet n'offrant pas nécessairement une qualité de service garantie. Seul le mode audio est obligatoire, les modes données et vidéo étant facultatifs; en cas de prise en charge de ces deux modes facultatifs, on doit pouvoir utiliser un mode de fonctionnement commun spécifié permettant l'interfonctionnement de tous les terminaux acceptant ce type de médias. Le réseau à commutation par paquets peut inclure des réseaux locaux, des réseaux d'entreprise, des réseaux métropolitains, des intraréseaux et des interréseaux (y compris l'Internet), des connexions point à point, un seul segment de réseau ou un interréseau de plusieurs segments aux topologies complexes. Les entités peuvent donc utiliser des configurations point à point, multipoint ou de diffusion. Elles peuvent fonctionner avec des terminaux sur le RNIS-LB, sur le RNIS-BE, sur des réseaux LAN offrant une qualité de service garantie, sur le RTGC et/ou sur des réseaux sans fil et peuvent être intégrées dans des ordinateurs personnels ou implémentées dans des dispositifs autonomes tels que des visiophones. Annexe J: Sécurisation des dispositifs d'extrémité simples.	CE 16
H.350.2	Architecture des services d'annuaire pour les systèmes H.235	Cette Recommandation décrit un schéma du protocole LDAP permettant de représenter des éléments de protocole H.235. Il s'agit d'une classe auxiliaire se rapportant à la Rec. UIT-T H.350, dont la plupart des fonctionnalités reposent sur cette architecture. Avant d'implémenter cette Recommandation, les réalisateurs d'applications devraient examiner en détail la Rec. UIT-T H.350. Les attributs associés comprennent les éléments suivants: identité H.235, mot de passe et certificat. Ces éléments peuvent être téléchargés en une extrémité en vue d'une configuration automatique, ou consultés par un portier en vue de la signalisation ou de l'authentification d'un appel. Le domaine d'application de cette Recommandation ne comprend pas les méthodes normatives applicables à l'utilisation de l'annuaire LDAP proprement dit ou des données qu'il contient. Ce schéma n'a pas pour objet de représenter tous les éléments de données possibles dans le protocole H.235, mais l'ensemble minimal nécessaire pour atteindre les objectifs de conception énumérés dans la Rec. UIT-T H.350.	CE 16
H.530	Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510	Cette Recommandation porte sur des procédures de sécurité dans les environnements H.323 avec mobilité, notamment pour la Rec. UIT-T H.510, qui décrit la mobilité pour les systèmes et services multimédias H.323. Elle décrit en détail les procédures de sécurité pour la Rec. UIT-T H.510. Jusque-là, les capacités de signalisation de la Rec. UIT-T H.235 dans ses versions 1 et 2 sont conçues pour prendre en charge la sécurité dans des environnements H.323 essentiellement sans mobilité. Dans ces environnements et dans les systèmes multimédias, une mobilité limitée est possible dans des zones de portier; la Rec. UIT-T H.323 en général et la Rec. UIT-T H.235 en particulier ne permettent qu'une prise en charge très réduite de la sécurité des utilisateurs et des terminaux mobiles lorsqu'ils passent d'un domaine à un autre et que de nombreuses entités interviennent dans un environnement réparti avec mobilité, par exemple. Les scénarios H.323 avec mobilité décrits dans la Rec. UIT-T H.510 relatifs à la mobilité des terminaux étant souples et dynamiques, ils constituent une situation nouvelle, notamment du point de vue de la sécurité. Lorsqu'ils passent d'un domaine à un autre, les terminaux mobiles et les utilisateurs H.323 doivent être authentifiés par le domaine étranger visité. De même, les utilisateurs mobiles souhaitent avoir la preuve de la véritable identité du domaine visité. En outre, il peut aussi être utile d'obtenir la preuve de l'identité des terminaux en plus de l'authentification des utilisateurs. Par conséquent, une authentification mutuelle de l'utilisateur et du domaine visité est absolument nécessaire, l'authentification de l'identité du terminal étant facultative. D'une manière générale, l'utilisateur mobile n'est connu que du domaine de rattachement dans lequel il est abonné et un mot de passe lui est attribué; ainsi, le domaine visité ne connaît pas cet utilisateur au départ. En tant que tel, le domaine visité ne partage aucune relation de sécurité établie avec l'utilisateur mobile et le terminal mobile. Concernant l'authentification et l'autorisation de l'utilisateur mobile et du terminal mobile, le domaine visité pourrait déléguer certaines tâches liées à la sécurité, telles que les contrôles d'autorisation ou la gestion des clés, au domaine de rattachement via des entités de réseau et de service intermédiaires. Pour cela, il faut sécuriser les communications et la gestion des clés entre le domaine visité et le domaine de rattachement. En principe, les environnements H.323 avec mobilité sont plus ouverts que les réseaux H.323 fermés, mais il faut bien évidemment sécuriser aussi de façon appropriée les tâches liées à la gestion des clés. Par ailleurs, il faut aussi protéger contre toute altération malveillante les communications intra et interdomaines de mobilité.	CE 16

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
J.93	Prescriptions d'accès conditionnel dans le réseau de distribution secondaire de la télévision numérique par câble	Cette Recommandation définit les prescriptions relatives à l'accès aux données et à la confidentialité des données afin de protéger les signaux de télévision numériques MPEG transmis sur les réseaux de télévision par câble entre la tête de réseau câblée et l'abonné ultime. Les algorithmes cryptographiques exacts utilisés dans ce processus ne figurent pas dans la Rec. UIT-T J.93 car ils sont déterminés à l'échelle régionale et/ou par les industries.	CE 9
J.96	Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Rec. UIT-T J.89	Cette Recommandation contient une norme commune relative à un système à accès conditionnel pour la transmission internationale longue distance de télévision numérique conformément au profil professionnel MPEG-2 (4:2:2). Elle décrit le système d'embrouillage de base compatible (BISS, *basic interoperable scrambling system*), fondé sur la spécification DVB-CSA et utilisant des clés fixes en langage clair appelées mots de session. Un autre mode rétrocompatible fournit un mécanisme supplémentaire permettant d'insérer des mots de session cryptés, tout en conservant, parallèlement, l'interopérabilité.	CE 9
J.112	Systèmes de transmission pour services interactifs de télévision par câble	Des services de télévision numérique ont été établis dans de nombreux pays et les avantages offerts par une extension de ces services destinée à fournir des services interactifs sont largement reconnus. Les systèmes de télédistribution par câble sont particulièrement adaptés à l'implémentation de services de données bidirectionnels et cette Recommandation complète et étend le domaine d'application de la Rec. UIT-T J.83 "Systèmes numériques multiprogrammes pour la distribution par câble de services de télévision, son et données" afin de permettre la transmission bidirectionnelle de données de services interactifs par système hybride fibre optique/câble coaxial. Cette Recommandation contient également plusieurs annexes qui tiennent compte des différents environnements de support existants. Il est recommandé d'utiliser les systèmes de cette Recommandation pour les services d'accès rapide à l'Internet ou les services interactifs de télévision par câble afin de réaliser des économies d'échelle et de faciliter l'interopérabilité. Les prescriptions de sécurité sont établies. Il est recommandé d'utiliser la Spécification de système de sécurité de transmission de données par câble (SP-DOCSS), la Spécification de module de sécurité amovible (SP-RSM) et la Spécification de sécurité fondamentale de transmission de données par câble (SP-BDS).	CE 9
J.160	Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems	Cette Recommandation contient le cadre architectural qui permettra aux opérateurs de télévision par câble d'acheminer des services à temps critique sur leurs réseaux qui ont été améliorés pour prendre en charge les câblo-modems. Les services de sécurité disponibles par l'intermédiaire de la couche des services essentiels de l'architecture IPCablecom sont l'authentification, le contrôle d'accès, l'intégrité, la confidentialité et la non-répudiation. Une interface de protocole IPCablecom peut employer zéro, un ou plusieurs de ces services afin de répondre à ses exigences de sécurité particulières. La sécurité IPCablecom répond comme suit aux exigences de sécurité de chaque interface de protocole constituante: • en identifiant le modèle de menace propre à chaque interface de protocole constituante; • en identifiant les services de sécurité (authentification, autorisation, confidentialité, intégrité et non-répudiation) requis pour répondre aux menaces identifiées; • en spécifiant le mécanisme de sécurité particulier qui assure les services de sécurité requis. Les mécanismes de sécurité comprennent aussi bien le protocole de sécurité (par exemple, IPsec, sécurité de couche RTP ou sécurité SNMPv3) que le protocole de gestion de clé sous-jacent (par exemple, IKE ou PKINIT/Kerberos).	CE 9
J.170	Spécification de la sécurité sur IPCablecom	Cette Recommandation définit l'architecture de sécurité, les protocoles, les algorithmes, les prescriptions fonctionnelles associées et des prescriptions techniques afin d'assurer la sécurité sur le réseau IPCablecom. Les *services de sécurité d'authentification, de contrôle d'accès, d'intégrité de message et de contenu support, de confidentialité et de non-répudiation* doivent être assurés conformément aux définitions données dans cette Recommandation pour chacune des interfaces d'élément de réseau.	CE 9

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
J.191	Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems	Cette Recommandation offre un ensemble de caractéristiques fondées sur le protocole IP qui peuvent être ajoutées à un câblo-modem afin de permettre aux câblo-opérateurs de fournir à leurs clients un ensemble supplémentaire de services améliorés comprenant la prise en charge de la qualité de service (QS) IPCablecom, une sécurité améliorée, des caractéristiques supplémentaires de gestion et d'approvisionnement, ainsi qu'un adressage et un traitement de paquets améliorés. Ces caractéristiques fondées sur le protocole IP résident dans un élément logique appelé *service portail* (*PS* ou *simplement portail*). Un câblo-modem contenant ces caractéristiques améliorées est un câblo-modem amélioré IP (IPCM, *IP-enhanced Cable Modem*) et c'est une implémentation de la classe de dispositifs HA J.190. Comme décrit dans la Rec. UIT-T J.190, la classe de dispositifs HA comporte à la fois la fonctionnalité de câblo-modem et la fonctionnalité de services portails. Le paragraphe 11 sur la sécurité définit les interfaces de sécurité, les protocoles et les exigences fonctionnelles nécessaires pour fournir de façon fiable les services IP par câble au service portail dans un environnement sécurisé. L'objet de toute technologie de sécurité est de protéger la valeur, qu'elle soit un flux de revenu ou un actif d'informations commercialisables d'un certain type. Les menaces contre ce revenu existent lorsqu'un utilisateur du réseau perçoit la valeur, dépense des efforts et de l'argent et invente une technique pour échapper aux paiements nécessaires. Annexe C: Dangers et mesures préventives.	CE 9
M.3010	Principes du réseau de gestion des télécommunications	Cette Recommandation définit les architectures – fonctionnelle, informationnelle et physique – d'un réseau de gestion des télécommunications (RGT) et leurs éléments fondamentaux. Elle décrit les relations existant entre les trois architectures et établit un cadre permettant d'établir les conditions à remplir pour la spécification des architectures physiques d'un RGT à partir des architectures fonctionnelles et informationnelles. Cette Recommandation propose un modèle de référence logique en vue de la stratification de la fonction de gestion, l'architecture logique répartie en couches (LLA, *logical layered architecture*). Elle établit les modalités à appliquer pour démontrer la conformité et l'observance de RGT aux fins d'interopérabilité. Les spécifications du RGT comprennent l'aptitude à garantir un accès sûr à l'information de gestion par les utilisateurs autorisés. Le RGT inclut des blocs fonctionnels pour lesquels la fonctionnalité de sécurité est assurée par des techniques de sécurité visant à protéger l'environnement du RGT afin de garantir la sécurité des informations échangées aux interfaces et résidant dans l'application de gestion. Principes et mécanismes de sécurité sont liés au contrôle des droits d'accès des utilisateurs du RGT aux informations associées aux applications du RGT.	CE 4
M.3016	Sécurité pour le plan de gestion	Cette Recommandation fournit un aperçu général et un cadre qui identifient les menaces de sécurité concernant un RGT et résume la manière dont les services de sécurité disponibles peuvent s'appliquer dans le cadre général de l'architecture fonctionnelle du RGT, telle que cette dernière est décrite dans la Rec. UIT-T M.3010. Elle est de nature générique et n'identifie ou ne concerne pas des prescriptions pour une interface de RGT spécifique. NOTE – La Rec. UIT-T M.3016 a été restructurée comme suit: • M.3016.0 – Sécurité pour le plan de gestion: aperçu général • M.3016.1 – Sécurité pour le plan de gestion: prescriptions de sécurité • M.3016.2 – Sécurité pour le plan de gestion: services de sécurité • M.3016.3 – Sécurité pour le plan de gestion: mécanisme de sécurité • M.3016.4 – Sécurité pour le plan de gestion: Formulaire des profils de sécurité	CE 4

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
M.3210.1	Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000	Cette Recommandation fait partie de la série de Recommandations *Services de gestion du réseau de gestion des télécommunications* qui contient une description des services de gestion, des objectifs et du contexte des aspects liés à la gestion des réseaux IMT-2000. Elle décrit un sous-ensemble des services de gestion de la sécurité afin d'offrir des prescriptions et une analyse de la gestion de la sécurité ainsi qu'un profil de *gestion des fraudes* dans un réseau mobile IMT-2000. L'accès est mis sur l'interface X entre deux fournisseurs de services et sur les services de gestion nécessaires entre ces deux fournisseurs afin que ceux-ci puissent détecter et prévenir toute forme de fraude grâce au système de collecte des informations de fraude (FIGS, *fraud information gathering system*), qui leur permet de surveiller un ensemble défini d'activités d'abonné afin de limiter leurs risques financiers face à des factures impayées conséquentes produites par des comptes d'abonné pendant que ces abonnés se trouvent en situation d'itinérance. Cette Recommandation s'appuie sur l'ensemble des fonctions identifiées dans la Rec. UIT-T M.3400 et définit des ensembles de fonctions, des fonctions et des paramètres nouveaux en y ajoutant des éléments sémantiques et limitations additionnelles.	CE 4
M.3320	Cadre général des prescriptions de gestion pour l'interface X du réseau de gestion des télécommunications	Cette Recommandation fait partie d'une série qui traite du transfert d'informations pour la gestion des réseaux et des services de télécommunication et seules certaines parties portent sur des aspects de sécurité. Cette Recommandation a pour objet de définir un cadre général couvrant toutes les prescriptions liées aux fonctions, aux services et aux réseaux pour l'échange d'informations entre Administrations via le réseau de gestion des télécommunications (RGT). Elle fournit également le cadre général concernant l'utilisation de l'interface X du RGT pour l'échange d'informations entre des Administrations, des exploitations reconnues, d'autres opérateurs de réseaux, des prestataires de services, des clients et d'autres entités. Elle spécifie les exigences de sécurité de l'interface X du RGT.	CE 4
M.3400	Fonctions de gestion du réseau de gestion des télécommunications	Cette Recommandation fait partie d'une série de Recommandations sur le réseau de gestion des télécommunications (RGT). Elle spécifie les fonctions de gestion et les ensembles de fonctions de gestion d'un RGT. Son contenu vient à l'appui de la base d'information de Tâche B (*rôles, ressources et fonctions RGT*), associée à la Tâche 2 (*description du contexte de gestion RGT*) indiquée dans la Rec. UIT-T M.3020. Lorsqu'on effectuera l'analyse d'un contexte de gestion RGT, il sera souhaitable d'envisager une utilisation maximale des ensembles de fonctions RGT proposés dans cette Recommandation. Cette Recommandation décrit la fonction de gestion de la sécurité prise en charge par le RGT.	CE 4
Q.293	Délais au bout desquels il convient de prendre des mesures de sécurité	Il s'agit d'un extrait du Livre Bleu, qui contient uniquement les § 8.5 (Délais au bout desquels il convient de prendre des mesures de sécurité) à 8.9 (Méthode de partage de la charge) de la Rec. UIT-T Q.293.	CE 4
Q.813	Elément de service d'application des transformations de sécurité pour l'élément de service d'opérations distantes (STASE-ROSE)	Cette Recommandation fournit des spécifications pour la prise en charge de transformations de sécurité, telles que *le chiffrement, le hachage, le scellé et la signature*, en se concentrant sur l'unité de données protocolaire (PDU, *protocol data unit*) de l'élément de service d'opérations distantes (ROSE, *remote operations service element*) considérée comme un tout. Les transformations de sécurité sont utilisées pour fournir divers services de sécurité tels que *l'authentification, la confidentialité, l'intégrité et la non-répudiation*. Cette Recommandation décrit une démarche pour la fourniture de transformations de sécurité qui est implémentée au niveau de la couche application et ne fait appel à aucune fonctionnalité spécifique de la sécurité dans l'une quelconque des couches sous-jacentes de la pile OSI. Elle permet d'améliorer la sécurité du RGT grâce à la prise en charge de transformations de sécurité pour les unités PDU ROSE et l'échange d'informations de sécurité connexes.	CE 4

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
Q.815	Spécification d'un module de sécurité pour la protection globale des messages	Cette Recommandation spécifie un module de sécurité facultatif à utiliser avec la Rec. UIT-T Q.814, *Spécification d'un agent interactif d'échange informatisé de données*, qui fournit des services de sécurité pour l'ensemble des unités de données protocolaires (PDU). Le module de sécurité prend notamment en charge la *non-répudiation de l'origine et de la réception*, ainsi que *l'intégrité* globale *des messages*.	CE 4
Q.817	Infrastructure des clés publiques du RGT – Profils des certificats numériques et des listes de révocation des certificats	Cette Recommandation expose la manière dont les certificats numériques et les listes de révocation de ces certificats peuvent être utilisés dans le RGT et définit les conditions d'utilisation de ces extensions des certificats et listes. Elle est destinée à faciliter l'interopérabilité entre éléments RGT utilisant l'infrastructure de clé publique (PKI, *public key infrastructure*) dans le cadre des fonctions de sécurité. L'objet de cette Recommandation est d'offrir un mécanisme interopérable et modulable pour *la distribution et la gestion de clés* à l'intérieur d'un RGT, de part et d'autre de toutes les interfaces, ainsi que pour la prise en charge d'un *service de non-répudiation* à travers l'interface X. Cette Recommandation concerne toutes les interfaces et applications du RGT. Elle est indépendante de la pile de protocoles de communication ou du protocole de gestion de réseau utilisé. Les ressources de l'infrastructure PKI peuvent être utilisées dans une grande étendue de fonctions de sécurité comme *l'authentification, l'intégrité, la non-répudiation et l'échange de clés* (Rec. UIT-T M.3016). Cette Recommandation ne spécifie cependant pas la façon dont il convient d'implémenter de telles fonctions, avec ou sans infrastructure PKI.	CE 4
Q.1531	Prescriptions de sécurité dans les TPU pour l'ensemble de services 1	Cette Recommandation spécifie les prescriptions de sécurité pour les télécommunications TPU concernant les communications entre l'utilisateur et le réseau ainsi qu'entre réseaux, qui s'appliquent à l'ensemble de services 1 des télécommunications TPU, tel qu'il est défini dans la Rec. UIT-T F.851. Cette Recommandation traite de toutes les caractéristiques de sécurité pour les télécommunications TPU utilisant des accès avec une signalisation multifréquence DTMF et les accès utilisateur basés sur la signalisation DSS 1 hors bande.	CE 11
Q.1741.1	Références IMT-2000 à la version 1999 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN)	Cette Recommandation contient des références aux spécifications suivantes du 3GPP relatives à la sécurité: *TS 21.133: Atteintes à la sécurité et exigences, TS 33.102: Architecture de la sécurité, TS 33.103: Directives d'intégration de la sécurité, TS 33.105: Exigences relatives à l'algorithme cryptographique, TS 33.106: Exigences d'interception licite, TS 33.107: Architecture et fonctions d'interception licite, TS 33.120: Objectifs et principes de sécurité.*	CE 19
Q.1741.2	Références IMT-2000 à la version 4 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN)	Cette Recommandation contient des références aux spécifications suivantes du 3GPP relatives à la sécurité: *TS 21.133: Sécurité 3G; atteintes à la sécurité et prescriptions, TS 22.048: Mécanismes de sécurité pour l'utilitaire d'application de module (U)SIM; étape 1, TS 22.101: Aspects du service; principes de service, TS 33.102: Sécurité 3G; architecture, TS 33.103: Sécurité 3G; directives d'intégration, TS 33.105: Prescriptions relatives à l'algorithme cryptographique, TS 33.106: Prescriptions d'interception licite, TS 33.107: Sécurité 3G; architecture et fonctions d'interception licite, TS 33.120: Objectifs et principes de sécurité, TS 33.200: Sécurité dans le domaine du réseau; protocole MAP, TS 35.205, .206, .207, et .208: Sécurité 3G; spécification de l'ensemble algorithmique MILENAGE.*	CE 19

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
Q.1741.3	Références IMT-2000 à la version 5 du réseau central UMTS issu du GSM	Cette Recommandation contient des références aux spécifications suivantes du 3GPP relatives à la sécurité: *TS 22.101: Aspects du service; principes de service, TS 33.102: Sécurité 3G; architecture, TS 33.106: Prescriptions d'interception licite, TS 33.107: Sécurité 3G; architecture et fonctions d'interception licite, TS 33.108: Sécurité 3G; interface de transfert pour l'interception licite, TS 33.200: Sécurité dans le domaine du réseau; protocole MAP, TS 33.203: Sécurité 3G; sécurité d'accès pour les services IP, TS 33.210: Sécurité; sécurité dans le domaine du réseau; sécurité de la couche de réseau IP, TS 35.205, .206, .207, .208 et .909: Sécurité 3G; spécification de l'ensemble algorithmique MILENAGE*.	CE 19
Q.1742.1	Références IMT-2000 au réseau central évolué ANSI-41 avec réseau d'accès cdma2000	Cette Recommandation associe les normes de réseau central publiées par des organisations de normalisation et les spécifications du projet 3GPP2 approuvées au 17 juillet 2001 pour le membre "Réseau central évolué ANSI-41 avec réseau d'accès cdma2000" de la famille des IMT-2000. Les spécifications du projet 3GPP2 approuvées jusqu'en juillet 2002 seront associées dans la future Rec. UIT-T Q.1742.2 aux normes de réseau central déjà publiées. L'interface radioélectrique, le réseau d'accès radioélectrique et les normes des organisations de normalisation pour ce membre de la famille des IMT-2000 sont associés dans la Rec. UIT-R M.1457. Les associations concernant d'autres membres de cette famille sont présentées dans les Recommandations UIT-T de la série Q.174x. Cette Recommandation réunit et associe en un seul texte, les normes de réseau central établies par plusieurs organisations de normalisation pour ce membre de la famille des IMT-2000.	CE 19
Q.1742.2	Références IMT-2000 (approuvées au 11 juillet 2002) au réseau central évolué ANSI-41 avec réseau d'accès cdma2000	Cette Recommandation associe les normes relatives au réseau central publiées par des organisations de normalisation (SDO, *standards development organization*) aux spécifications 3GPP2, approuvées au 11 juillet 2002, du "Réseau central évolué ANSI-41 avec réseau d'accès cdma2000" qui fait partie de la famille des IMT-2000. Les spécifications 3GPP2 approuvées au 17 juillet 2001 ont été associées dans la Rec. UIT-T Q.1742.1 aux normes de réseau central déjà publiées. Les spécifications 3GPP2 approuvées jusqu'en juillet 2003 seront associées dans la future Rec. UIT-T Q.1742.3 aux normes de réseau central déjà publiées. L'interface radioélectrique, le réseau d'accès radioélectrique et les normes des organisations de normalisation pour ce membre de la famille des IMT-2000 sont associés dans la Rec. UIT-R M.1457. Les associations concernant d'autres membres de cette famille sont présentées dans les Recommandations UIT-T de la série Q.174x. Cette Recommandation réunit et associe en un seul texte, les normes régionales relatives au réseau central de ce membre de la famille des IMT-2000.	CE 19
Q.1742.3	Références IMT-2000 (approuvées au 30 juin 2003) au réseau central évolué ANSI-41 avec réseau d'accès cdma2000	Les spécifications techniques suivantes citées dans la Rec. UIT-T Q.1742.3 portent sur des aspects de sécurité: *Spécifications intersystèmes:* N.S0003-0 User Identity Module (Version 1.0; avril 2001) N.S0005-0 Cellular Radiotelecommunications Intersystem Operations (Version 1.0; pas de date) N.S0009-0 IMSI (Version 1.0; pas de date) N.S0010-0 Advanced features in Wideband Spread Spectrum Systems (Version 1.0; pas de date) N.S0011-0 OTASP and OTAPA (Version 1.0; pas de date) N.S0014-0 Authentication Enhancements (Version 1.0; pas de date) N.S0018 TIA/EIA-41-D Prepaid Charging (Version 1.0.0; 14 juillet 2000) N.S0028 Network Interworking Between GSM MAP and ANSI-41 MAP Rev. B Revision: 0 (Version 1.0.0; avril 2002) *Spécifications applicables aux données en mode paquet:* P.S0001-A Wireless IP Network Standard (Version 3.0.0; 16 juillet 2001) P.S0001-B Wireless IP Network Standard (Version 1.0.0; 25 octobre 2002)	CE 19

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
		Spécifications des aspects services et système: S.R0005-B Network Reference Model for cdma2000 Spread Spectrum Systems Revision: B (Version 1.0; 16 avril 2001) S.R0006 Wireless Features Description Revision: 0 (Version 1.0.0; 13 décembre 1999) S.R0009-0 User Identity Module (Version 1.0; Stage 1) Revision: 0 (13 décembre 1999) S.R0018 Pre-Paid Charging (Version 1.0.0; Stage 1) Revision: 0 (13 décembre 1999) S.R0019 Location-Based Services System (Version 1.0.0; LBSS) Stage 1 Description (22 septembre 2000) S.R0032 Enhanced Subscriber Authentication (Version 1.0; ESA) and Enhanced Subscriber Privacy (ESP) (6 décembre 2000) S.R0037-0 IP Network Architecture Model for cdma2000 Spread Spectrum Systems (Version 2.0; 14 mai 2002) S.R0048 3G Mobile Equipment Identifier (Version 1.0; MEID) (10 mai 2001) S.S0053 Common Cryptographic Algorithms (Version 1.0; 21 janvier 2002) S.S0054 Interface Specification for Common Cryptographic Algorithms (Version 1.0; 21 janvier 2002) S.S0055 Enhanced Cryptographic Algorithms (Version 1.0; 21 janvier 2002) S.R0058 IP Multimedia Domain System Requirements (Version 1.0; 17 avril 2003) S.R0059 Legacy MS Domain – Step 1 System Requirements (Version 1.0; 16 mai 2002) S.R0066-0 IP Based Location Services Stage 1 Requirements (Version 1.0; 17 avril 2003) S.R0071 Legacy System Packet Data Surveillance Requirements Stage 1 Requirements (Version 1.0; 18 avril 2002) S.R0072 All IP Packet Data Surveillance Requirements Stage 1 Requirements (Version 1.0; 18 avril 2002) S.R0073 Internet Over-the-Air Handset Configuration Management (Version 1.0; IOTA) Stage 1 (11 juillet 2002) S.S0078-0 Common Security Algorithms (Version 1.0; 12 décembre 2002)	
T.30	Procédures pour la transmission de documents par télécopie sur le réseau téléphonique général commuté	L'Annexe G contient des procédures pour la transmission sécurisée de documents de télécopie du Groupe 3 utilisant les systèmes HKM et HFX. L'Annexe H porte sur la sécurisation de la télécopie G3 sur la base de *l'algorithme* RSA.	CE 16
T.36	Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3	Cette Recommandation définit les deux solutions techniques indépendantes, fondées sur les algorithmes HKM/HFX40 et *l'algorithme RSA*, qui peuvent être appliquées afin d'assurer la sécurité des transmissions par télécopie.	CE 16
T.123 Annexe B	Connexions de transport étendues	Cette Annexe à la Rec. UIT-T T.123 révisée décrit un *protocole de négociation de connexion* (CNP, *connection negotiation protocol*) qui permet de négocier les capacités de sécurité. Le mécanisme de sécurité appliqué inclut divers moyens permettant d'assurer la sécurité de réseau et de transport nœud par nœud (par exemple TLS/SSL, IPSEC sans IKE ou *gestion de clés manuelle*, X.274/ ISO TLSP et GSS-API).	CE 16
T.503	Profil d'application de document pour le transfert de documents de télécopie du Groupe 4	Cette Recommandation définit un profil d'application de document qui peut être utilisé par n'importe quel service télématique. Elle a pour objet de spécifier un format d'échange applicable à l'échange de documents de télécopie du Groupe 4 ne contenant que des graphiques en points. Les documents sont échangés sous une forme formatée, qui permet au destinataire d'afficher et d'imprimer le document comme l'a prévu l'expéditeur.	CE 16

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
T.563	Caractéristiques des télécopieurs du Groupe 4	Cette Recommandation définit les aspects généraux des télécopieurs du Groupe 4 ainsi que l'interface avec le réseau physique.	CE 16
T.611	Interface de communication programmable APPLI/COM pour les services de télécopie du Groupe 3, de télécopie du Groupe 4, télétex, télex, de messagerie électronique et de transfert de fichiers	Cette Recommandation définit l'interface de communication programmable (PCI) appelée "APPLI/COM", assurant un accès unifié à différents services de télécommunication tels que le service de télécopie du Groupe 3 ou d'autres services de télématique. Elle décrit la structure et le contenu des messages ainsi que le procédé d'échange entre deux entités (à savoir l'application locale et l'application de communication). Toute communication est précédée par un processus d'ouverture de session et se termine par un processus de fermeture de session. Ces deux processus facilitent l'implémentation de schémas de sécurité qui sont particulièrement importants dans les systèmes multi-utilisateurs. Ils permettent aussi d'implémenter des mécanismes de sécurité entre l'application locale et l'application de communication. Cette Recommandation constitue une API (interface de programmation d'application) de haut niveau qui donne aux concepteurs d'applications un puissant moyen de commande et de surveillance des activités de télécommunication.	CE 16
X.217	Technologies de l'information – Interconnexion des systèmes ouverts – Définition de service applicable à l'élément de service de contrôle d'association	Cette Recommandation définit les services applicables à l'élément de service de contrôle d'association (ACSE, *association control service element*) nécessaires au contrôle d'association d'application dans un environnement OSI. L'ACSE prend en charge deux modes de communication: connexion et sans connexion. Trois unités fonctionnelles sont définies dans l'ACSE. L'*unité fonctionnelle noyau* obligatoire sert à établir des associations d'application et à y mettre fin. L'ACSE inclut deux unités fonctionnelles facultatives, l'une d'elles étant l'unité fonctionnelle *authentification*, qui fournit des moyens supplémentaires permettant l'échange d'informations destinées à l'authentification lors de l'établissement d'une association sans ajouter de services. On peut recourir aux *facilités d'authentification* ACSE pour disposer d'une catégorie limitée de *méthodes d'authentification*. L'Amendement 1 permet d'assurer la prise en charge des mécanismes d'authentification en mode sans connexion.	CE 17
X.227	Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: spécification du protocole.	Cette Spécification de protocole définit les procédures applicables à des instances de communication entre des systèmes qui désirent s'interconnecter dans un environnement OSI en mode connexion, c'est-à-dire un protocole en mode connexion applicable à l'élément de service d'application pour le contrôle d'association d'application, l'élément de service de contrôle d'association (ACSE). Cette Spécification de protocole inclut l'*unité fonctionnelle noyau* qui est utilisée pour établir les associations d'application et y mettre fin. L'*unité fonctionnelle d'authentification* offre des fonctions supplémentaires qui permettent l'échange d'informations destinées à assurer l'*authentification* pendant l'établissement de l'association sans que soient ajoutés de nouveaux services. Les *fonctions d'authentification* de l'élément ACSE peuvent être utilisées pour la prise en charge d'une classe limitée de *méthodes d'authentification*. L'unité fonctionnelle de négociation du contexte d'application offre des fonctions supplémentaires qui permettent le choix du contexte d'application pendant l'établissement de l'association. Cette Spécification de protocole comprend une annexe qui décrit une machine protocolaire, appelée machine protocolaire de contrôle d'association (ACPM, *association control protocol machine*), en termes d'une table d'états. Elle comprend aussi une annexe qui décrit un mécanisme d'authentification simple utilisant un mot de passe avec une appellation AE et destiné à l'usage du public et qui contient aussi un exemple de *spécification de mécanisme d'authentification*. Le nom suivant (de type de données ASN.1 OBJECT IDENTIFIER) est affecté à ce mécanisme d'authentification: {joint-iso-itu-t(2) association-control(2) authentication-mechanism(3) password-1(1)}. Pour ce mécanisme d'authentification, le mot de passe est la valeur d'authentification. Le type de données de valeur d'authentification doit être "chaîne graphique".	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.237	Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode sans connexion pour l'élément de service de contrôle d'association: Spécification du protocole	L'Amendement 1 à cette Recommandation introduit le marqueur d'extension ASN.1 dans le module décrivant le protocole. Il améliore également la spécification du protocole sans connexion pour l'ACSE afin de permettre l'acheminement de paramètres d'authentification dans l'unité APDU A-UNIT-DATA.	CE 17
X.257	Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode sans connexion de l'élément de service de contrôle d'association: formulaire de déclaration de conformité d'une instance de protocole	Cette Recommandation décrit le formulaire de déclaration de conformité d'une instance de protocole (PICS, *protocol implementation conformance statement*) applicable au protocole en mode sans connexion de l'élément de service de contrôle d'association (ACSE, *association control service element*) qui est spécifié dans la Rec. UIT-T X.237. Le formulaire PICS représente, sous la forme de tableaux, les éléments obligatoires et optionnels du protocole en mode sans connexion de l'élément de service ACSE. Le formulaire PICS est utilisé pour indiquer les caractéristiques et options d'une instance particulière du protocole en mode sans connexion de l'élément de service ACSE.	CE 17
X.272	Compression et secret des données dans les réseaux à relais de trames	Cette Recommandation définit le service de compression et de secret des données dans les réseaux à relais de trames, y compris la négociation et l'encapsulation de la compression de données, de la *compression sécurisée de données*, de *l'authentification et du cryptage* en relais de trames. La présence d'un *service de compression* de données dans un réseau augmentera le débit effectif de celui-ci. La demande en transmission de données sensibles sur des réseaux publics nécessite des ressources permettant d'assurer le secret de ces données. Afin d'obtenir des taux de compression optimaux, il est essentiel de comprimer les données avant de les crypter. Il est donc souhaitable d'offrir, dans la spécification du *service de compression des données*, des ressources permettant de négocier également des *protocoles de cryptage des données*. Etant donné que la tâche de compression puis de cryptage des données exige beaucoup de ressources de calcul, certains protocoles ont été proposés afin d'assurer simultanément la *compression des données et leur cryptage* (*compression de données sécurisée*). Les protocoles de compression de données sont fondés sur le protocole de commande de liaison PPP (IETF RFC 1661) et sur le protocole de commande de cryptage PPP (IETF RFC 1968 et 1969). Cette Recommandation s'applique aux trames d'information non numérotée (UI, *unnumbered information*) encapsulées conformément à l'Annexe E/Q.933. Elle traite de la compression et du secret des données sur connexions virtuelles permanentes (PVC, *permanent virtual connection*) comme sur connexions virtuelles commutées (SVC, *switched virtual connection*).	CE 17
X.273	Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de sécurité de la couche Réseau	Cette Recommandation spécifie le protocole pouvant prendre en charge les *services d'intégrité, de confidentialité, d'authentification et de contrôle d'accès* identifiés dans le modèle de sécurité OSI comme applicables aux protocoles de couche réseau en mode connexion et en mode sans connexion. Le protocole prend en charge ces services au moyen de *mécanismes cryptographiques, d'étiquetages de sécurité et d'attributs* (*clés de chiffrement* par exemple) préétablis par la gestion de sécurité.	CE 17
X.274	Technologies de l'information – Télécommunication et échange d'informations entre systèmes – Protocole de sécurité de la couche transport	Cette Recommandation spécifie le protocole pouvant prendre en charge les *services d'intégrité, de confidentialité, d'authentification et de contrôle d'accès* identifiés dans le modèle de sécurité OSI comme relevant de la couche transport. Le protocole prend en charge ces services au moyen *de mécanismes cryptographiques, d'étiquetages de sécurité et d'attributs* (*clés de chiffrement* par exemple) préétablis par la gestion de sécurité.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.400/ F.400	Aperçu général du système et du service de messagerie	Cette Recommandation définit les éléments de service du système de messagerie (MHS) pour les services de sécurité suivants entre deux agents d'utilisateur, entre deux agents de transfert de messages, entre un agent d'utilisateur et un agent de transfert de message ainsi qu'entre un agent d'utilisateur et une mémoire de messages: *confidentialité, intégrité, authentification, non-répudiation et contrôle d'accès*, services identifiés comme se rapportant à la couche application. (Voir F.400)	CE 17
X.402	Technologies de l'information – Systèmes de messagerie: Architecture globale	Cette Recommandation spécifie les procédures de sécurité et les identificateurs d'objet à utiliser dans les protocoles MHS pour réaliser les services *de confidentialité, d'intégrité, d'authentification, de non-répudiation et de contrôle d'accès* identifiés comme se rapportant à la couche application.	CE 17
X.411	Technologie de l'information – Systèmes de messagerie – Système de transfert de messages: définition et procédures du service abstrait	Cette Recommandation spécifie les mécanismes et les procédures prenant en charge *les services de confidentialité, d'intégrité, d'authentification et de non-répudiation* identifiés comme se rapportant à la couche application. Le protocole prend en charge ces services en utilisant *des mécanismes cryptographiques, un étiquetage de sécurité et des signatures numériques*, présentés dans la Rec. UIT-T X.509. Cette Recommandation spécifie un protocole qui utilise des *techniques de chiffrement asymétrique*, mais les *techniques de chiffrement symétrique* sont également prises en charge.	CE 17
X.413	Technologies de l'information – Systèmes de messagerie: mémoire de messages: définition du service abstrait	Cette Recommandation spécifie les mécanismes, le protocole et les procédures prenant en charge *les services d'intégrité, de contrôle d'accès, d'authentification et de non-répudiation* identifiés comme se rapportant à la couche application. Le protocole prend en charge ces services pour le compte de l'utilisateur direct de la mémoire de messages.	CE 17
X.419	Technologies de l'information – Systèmes de messagerie: Spécification des protocoles	Cette Recommandation spécifie les procédures et les contextes d'application permettant d'assurer un accès sécurisé aux entités et utilisateurs distants du système de messagerie grâce à la prise en charge *des services d'authentification et de contrôle d'accès* identifiés comme se rapportant à la couche application.	CE 17
X.420	Technologies de l'information – Systèmes de messagerie: système de messagerie de personne à personne	Cette Recommandation spécifie les mécanismes, le protocole et les procédures applicables à l'échange d'objets entre utilisateurs de la messagerie de personne à personne ou agents d'utilisateur pour le compte de l'utilisateur direct. Les services de sécurité pris en charge sont *l'intégrité, la confidentialité, l'authentification et le contrôle d'accès* identifiés comme se rapportant à la couche application.	CE 17
X.435	Technologies de l'information – Systèmes de messagerie: système de messagerie par échange informatisé de données	Cette Recommandation spécifie les mécanismes, le protocole et les procédures applicables à l'échange d'objets entre agents d'utilisateur de l'échange informatisé de données (EDI, *electronic data interchange*) pour le compte de l'utilisateur direct. Les services de sécurité pris en charge sont *l'intégrité, la confidentialité, l'authentification et le contrôle d'accès* identifiés comme se rapportant à la couche application.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.440	Systèmes de messagerie: système de messagerie vocale	Cette Recommandation spécifie les mécanismes, le protocole et les procédures applicables à l'échange d'objets entre agents d'utilisateur de la messagerie vocale pour le compte de l'utilisateur direct. Les services de sécurité pris en charge sont *l'intégrité, la confidentialité, l'authentification et le contrôle d'accès* identifiés comme se rapportant à la couche application.	CE 17
X.500	Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services	Cette Recommandation a été élaborée, ainsi que d'autres Recommandations, pour faciliter l'interconnexion des systèmes de traitement de l'information et permettre ainsi d'assurer des services d'annuaire. L'ensemble de tous ces systèmes, avec les informations d'annuaire qu'ils contiennent, peut être considéré comme un tout intégré, appelé annuaire. Les informations de l'annuaire, appelées collectivement base d'informations d'annuaire (DIB, *directory information base*), sont généralement utilisées pour faciliter la communication entre, avec ou à propos d'objets tels que des entités d'application, des personnes, des terminaux et des listes de distribution. L'annuaire joue un rôle important dans l'interconnexion des systèmes ouverts, dont le but est de permettre, moyennant un minimum d'accords techniques en dehors des normes d'interconnexion proprement dites, l'interconnexion des systèmes de traitement de l'information. Cette Recommandation présente et modélise les concepts de l'annuaire et de la base DIB. Elle donne un aperçu général des services et des possibilités qu'ils offrent. D'autres Recommandations utilisent ces modèles pour définir le service abstrait fourni par l'annuaire et pour spécifier les protocoles permettant d'obtenir ou de diffuser ce service. Cette Recommandation spécifie l'annuaire et ses caractéristiques de sécurité.	CE 17
X.501	Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles	Cette Recommandation fournit un certain nombre de modèles relatifs à l'annuaire comme cadre de travail pour les autres Recommandations UIT-T de la série X.500. Ces modèles sont le modèle (fonctionnel) général, le modèle d'autorité administrative, les modèles génériques d'informations d'annuaire fournissant à l'utilisateur d'annuaire et à l'utilisateur administratif des vues d'informations d'annuaire, les modèles génériques d'agent de système d'annuaire (DSA, *directory system agent*) et d'informations d'agent DSA, un cadre de travail opérationnel et un modèle de sécurité. Cette Recommandation spécifie l'utilisation du cadre général des certificats de clé publique et d'attribut X.509 de l'annuaire.	CE 17
X.509	Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Cadre d'authentification (édition de 1993 – *deuxième édition/ version*). Cadre d'authentification (édition de 1997 – *troisième édition/ version*). Cadre général des certificats de clé publique et d'attribut (édition de 2000 – *quatrième édition/ version*). Cadre général des certificats de clé publique et d'attribut (édition de 2005 – *cinquième édition/version*)	Cette Recommandation définit un cadre général des certificats de clé publique et d'attribut ainsi qu'un cadre pour la fourniture de services d'authentification de l'annuaire au bénéfice de ses utilisateurs. Elle décrit deux niveaux d'authentification, l'*authentification simple* utilisant un mot de passe pour vérifier l'identité déclarée et l'*authentification forte* nécessitant des justificatifs créés au moyen de méthodes de chiffrement. L'authentification simple fournit une certaine protection contre les accès non autorisés, mais seule l'authentification forte devrait être utilisée pour fournir la base de services fiables. Les cadres définis peuvent être utilisés pour définir un profil d'application d'*infrastructures de clé publique* (PKI) et d'*infrastructures de gestion de privilège* (PMI). Le cadre des certificats de clé publique comprend la spécification des objets de données utilisés pour représenter les certificats proprement dits ainsi que les notifications de révocation de certificats émis et auxquels il ne doit plus être fait confiance. Il définit certains composants critiques d'une infrastructure de clé publique (PKI), mais pas la totalité d'une telle infrastructure. Toutefois, il constitue une base permettant d'édifier des infrastructures PKI complètes et leurs spécifications. Le cadre des certificats d'attribut contient la spécification des *objets de données* utilisés pour représenter les certificats proprement dits, ainsi que les *notifications de révocation* de certificat émis auxquels il ne doit plus être fait confiance. Il définit certains composants critiques d'une infrastructure de gestion de privilège (PMI), mais pas la totalité d'une telle infrastructure. Toutefois, il constitue une base permettant d'édifier des infrastructures PMI complètes et leurs spécifications. Sont définis également les *objets d'informations* permettant de stocker les objets d'infrastructure PKI et PMI dans l'annuaire et de comparer des valeurs présentées avec les valeurs stockées.	CE 17
X.519	Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification des protocoles	Cette Recommandation spécifie les procédures et les contextes d'application permettant d'assurer un accès sécurité au cours du rattachement d'entités d'annuaire.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.680	Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base	Cette Recommandation spécifie une notation dite notation de syntaxe abstraite numéro un (ASN.1) pour la définition de la syntaxe de données informationnelles. Elle définit un certain nombre de types de données simples et spécifie une notation pour y faire référence et en spécifier les valeurs. La notation ASN.1 peut être utilisée chaque fois qu'il est nécessaire de définir la syntaxe abstraite d'informations sans imposer de contrainte sur la manière de coder ces informations en vue de leur transmission. La notation ASN.1 sert à définir les types de données, les valeurs et les contraintes imposées à ces types. Cette Recommandation définit un certain nombre de types simples, avec leurs étiquettes, et spécifie une notation pour faire référence à ces types et pour spécifier leurs valeurs; définit des mécanismes pour construire de nouveaux types à partir de types plus élémentaires, et spécifie une notation pour définir de tels types, leur affecter des étiquettes, et en spécifier les valeurs; définit (par référence à d'autres Recommandations) les jeux de caractères à utiliser en notation ASN.1. Un type de donnée (en abrégé, un type) est une catégorie informationnelle (une information numérique, textuelle, iconographique ou vidéo par exemple). Une valeur de donnée (en abrégé une valeur) est une instance d'un tel type. Cette Recommandation définit plusieurs types de base et les valeurs qui leur correspondent, ainsi que les règles pour les combiner en types et valeurs plus complexes. Dans certaines architectures de protocole, chaque message est spécifié comme la valeur binaire d'une séquence d'octets. Les rédacteurs de normes ont cependant besoin de définir des types de données vraiment complexes afin d'exprimer leurs messages, quelle que soit leur représentation binaire. Afin de spécifier ces types de données, ils ont besoin d'une notation qui ne détermine pas nécessairement la représentation de chaque valeur, ce qui est le cas de la notation de syntaxe abstraite numéro un (ASN.1). Cette notation est complétée par la spécification d'un ou de plusieurs algorithmes appelés règles de codage, qui déterminent la valeur des octets exprimant la sémantique applicative (appelée syntaxe de transfert). NOTE – Les séries de Recommandations sur l'ASN.1 (et en particulier les règles de codage distinctives et canoniques de l'ASN.1) ont été largement utilisées dans bon nombre de normes et de Recommandations liées à la sécurité. En particulier, la Rec. UIT-T H.323 et les séries X.400 et X.500 dépendent fortement de la notation ASN.1. Ces Recommandations ont constitué et continuent de constituer des éléments importants pour les travaux lies à la sécurité.	CE 17
X.681	Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels	Cette Recommandation spécifie la notation ASN.1 qui permet de définir les classes d'objets informationnels ainsi que les objets informationnels proprement dits et de leur donner des noms de référence. En effet, elle établit une notation permettant de spécifier les classes d'objets informationnels, les objets informationnels et les ensembles d'objets informationnels. Une classe d'objets informationnels définit la forme d'un tableau conceptuel (un ensemble d'objets informationnels), une colonne étant attribuée à chaque champ dans la classe d'objets informationnels, et chaque ligne complète définissant un objet informationnel. Le concepteur d'applications est fréquemment appelé à concevoir un protocole destiné à fonctionner avec un certain nombre d'instances d'une certaine classe d'objets informationnels, ces instances pouvant être définies par diverses entités au cours du temps. Comme exemple de classe d'objets informationnels, on peut citer les "opérations" du service d'opérations distantes (ROS, *remote operations service*) et les "attributs" de l'annuaire de l'OSI. Cette Recommandation spécifie une notation permettant de définir des classes d'objets informationnels ainsi que des objets informationnels individuels et des ensembles d'objets informationnels et de leur attribuer des noms de référence. Voir NOTE ci-dessus (X.680).	CE 17
X.682	Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes	Cette Recommandation fait partie de la notation de syntaxe abstraite numéro un (ASN.1, *abstract syntax notation one*); elle indique la notation à utiliser pour spécifier les contraintes définies par l'utilisateur, les contraintes tabulaires et les contraintes de contenu. Cette Recommandation décrit la notation ASN.1 à utiliser, dans le cas général, pour spécifier les contraintes et les exceptions par lesquelles on peut limiter les valeurs d'un type de données structuré. Elle contient aussi les éléments de signalisation à utiliser en cas de transgression d'une contrainte. Les concepteurs d'applications ont besoin d'une notation pour définir un type de données structuré servant à acheminer leur sémantique. Une notation est aussi nécessaire pour appliquer des contraintes aux valeurs qui peuvent apparaître. De telles contraintes limitent la plage de valeurs de certains composants, soit à l'aide d'un ensemble d'objets informationnels spécifié afin de définir une contrainte sur un composant "ObjectClassFieldType" (type de champ de classe d'objets), soit à l'aide de la notation "AtNotation" afin de spécifier une relation entre des composants. Voir NOTE ci-dessus (X.680).	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.683	Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un	Cette Recommandation, qui fait partie de la notation de syntaxe abstraite numéro un (ASN.1, *abstract syntax notation one*), définit la notation pour le paramétrage des spécifications ASN.1. En effet, elle définit les dispositions relatives aux noms de référence paramétrés et à l'affectation paramétrée pour des types de données qui sont utiles au concepteur quand il établit des spécifications dont certains aspects, qui ne sont pas encore définis à ce stade, le seront ultérieurement pour aboutir à la définition complète d'une syntaxe abstraite. Les concepteurs d'applications doivent rédiger des spécifications dont certains aspects ne sont pas définis. Ces aspects seront définis ultérieurement par un ou plusieurs autres groupes (chacun à sa manière), afin de produire une spécification entièrement définie servant à définir une syntaxe abstraite (une pour chaque groupe). Dans certains cas, certains aspects de la spécification (par exemple, des limites) peuvent ne pas être définis même au moment de la définition de la syntaxe abstraite et seront complétés par la spécification de profils normalisés au plan international ou de profils fonctionnels fournis par un autre organisme. Voir NOTE ci-dessus (X.680).	CE 17
X.690	Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives	Cette Recommandation spécifie un ensemble de règles de codage de base (BER, *basic encoding rules*) applicables aux valeurs des types définis au moyen de la notation ASN.1, autrement dit des règles qui peuvent être utilisées pour spécifier une syntaxe de transfert pour des valeurs appartenant à des types définis au moyen de la notation spécifiée dans la série X.680 de la Rec. UIT-T, appelée syntaxe abstraite numéro un ou ASN.1. L'application de ces règles de codage produit une syntaxe de transfert pour de telles valeurs. Il est implicitement entendu que ces règles de codage servent également au décodage. En effet, ces règles de codage de base s'appliquent également au décodage d'une telle syntaxe de transfert pour identifier les valeurs de données transférées. Cette Recommandation spécifie également un ensemble de règles canoniques et distinctives qui restreignent le codage des valeurs à une seule des possibilités autorisées par les règles de codage de base. En effet, elle définit également un ensemble de règles de codage distinctives (DER, *distinguished encoding rules*) et un ensemble de règles de codage canoniques (CER, *canonical encoding rules*) qui permettent tous deux de déclarer des contraintes sur les règles de codage de base (BER). La principale différence entre ces deux ensembles de règles est que les DER utilisent des formes de codage de longueur définie alors que les CER utilisent les formes de longueur indéfinie. Les DER sont mieux adaptées au codage des petites valeurs, et les CER à celui des grandes valeurs. Il est implicitement entendu que ces règles de codage servent également au décodage. Voir NOTE ci-dessus (X.680).	CE 17
X.691	Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage compact	La série X.680 de la Rec. UIT-T décrit la notation de syntaxe abstraite numéro un (ASN.1) qui permet de définir les messages échangés par des applications homologues. Cette Recommandation décrit un ensemble de règles de codage applicables aux valeurs de tous les types ASN.1. Ces règles donnent une représentation plus compacte que celle que l'on peut obtenir au moyen des règles de codage de base et de leurs dérivées (décrites dans la Rec. UIT-T X.690). En effet, cette Recommandation spécifie un ensemble de règles de codage compact qui peuvent être utilisées pour élaborer une syntaxe de transfert applicable à des valeurs de types définis dans la Rec. UIT-T X.680. Ces règles de codage compact sont également applicables au décodage d'une telle syntaxe de transfert afin d'identifier les valeurs de données qui sont transférées. Plusieurs ensembles de règles de codage peuvent être appliqués à des valeurs de types ASN.1. Ces règles de codage compact (PER, *packed encoding rules*) sont ainsi dénommées parce qu'elles donnent une représentation plus compacte que celle que l'on peut obtenir au moyen des règles de codage de base (BER, *basic encoding rules*) et de leurs dérivées, décrites dans la Rec. UIT-T X.690. Voir NOTE ci-dessus (X.680).	CE 17
X.692	Technologies de l'information – Règles de codage ASN.1: spécification de la notation de contrôle de codage (ECN) Annexe E: Prise en charge des codages de Huffman	Cette Recommandation définit la notation de contrôle de codage (ECN, *encoding control notation*) utilisée afin de spécifier les codages de types ASN.1 ou de parties de types qui diffèrent de ceux qui sont fournis par les règles de codage normalisées telles que les règles de codage de base (BER) et les règles de codage compact (PER). Elle offre plusieurs mécanismes pour une telle spécification. Elle offre également le moyen de relier la spécification de codages aux définitions des types auxquels elles doivent être appliquées. La notation ECN peut être utilisée pour coder tous les types d'une spécification ASN.1, mais peut également être utilisée avec les règles de codage normalisées telles que BER ou PER afin de spécifier seulement le codage de types qui ont des exigences spéciales. Un type ASN.1 spécifie un ensemble de valeurs abstraites. Les règles de codage spécifient la représentation de ces valeurs abstraites sous la forme d'une série de bits. Voir NOTE ci-dessus (X.680).	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.693	Technologies de l'information – Règles de codage ASN.1: règles de codage XML (XER)	La publication de la notation de syntaxe abstraite numéro un (ASN.1) est devenue la notation généralement utilisée pour définir les messages échangés par des applications homologues. Cette Recommandation spécifie les règles de codage qui peuvent être appliquées pour coder des valeurs de types ASN.1 au moyen du langage de balisage extensible (XML). En effet, elle définit un ensemble de règles de codage XML de base qui peuvent être utilisées pour élaborer une syntaxe de transfert applicable à des valeurs de types définis dans la série X.680 de Recommandations UIT-T. Elle définit également un ensemble de règles de codage XML canonique qui impose des limites aux règles de codage XML de base de manière à produire un codage exclusif pour chaque valeur ASN.1. La spécification de ces règles de codage suppose implicitement que ces règles pourront aussi être utilisées pour le décodage. L'application de ces règles de codage produit une syntaxe de transfert pour de telles valeurs. La spécification de ces règles de codage suppose implicitement que ces règles pourront aussi être utilisées pour le décodage. Plusieurs ensembles de règles de codage peuvent être appliqués à des valeurs de types ASN.1. Cette Recommandation définit deux ensembles de règles de codage utilisant le langage de balisage extensible (XML, *extensible markup language*). Appelés règles de codage XML (XER, *XML encoding rules*) pour l'ASN.1, ces deux ensembles produisent un document conforme W3C XML 1.0. Le premier est appelé règles de codage XML de base, le second règles de codage XML canonique car celles-ci ne permettent de coder une valeur ASN.1 que d'une seule manière (les règles de codage canonique sont généralement utilisées pour des applications utilisant des fonctions liées à la sécurité telles que des signatures numériques).	CE 17
X.733	Technologies de l'information – Interconnexion de systèmes ouverts – Gestion-systèmes: fonction de signalisation des alarmes	Cette Recommandation définit une fonction de gestion des systèmes interactive qui peut être utilisée par un processus d'application dans le contexte d'une gestion centralisée ou décentralisée. Elle définit une fonction qui se compose de définitions génériques, de services et d'unités fonctionnelles et qui s'inscrit dans la couche application. Les notifications d'alarme définies par cette fonction fournissent l'information dont peut avoir besoin le gestionnaire des systèmes pour réagir selon les conditions d'exploitation et la qualité de service propre à un système.	CE 4
X.735	Technologie de l'information – Interconnexion de systèmes ouverts – Gestion-systèmes: fonction de commande des registres de consignation	Cette Recommandation définit une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée aux fins de la gestion des systèmes. Elle définit la fonction de commande des registres de consignation (fonction de commande de consignation) au moyen de services et de deux unités fonctionnelles. Cette fonction se situe dans la couche application.	CE 4
X.736	Technologies de l'information – Interconnexion de systèmes ouverts – Gestion-systèmes: fonction de signalisation des alarmes de sécurité	Cette Recommandation définit la fonction de signalisation des alarmes de sécurité. Cette fonction est une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée pour échanger des informations destinées à la gestion des systèmes. Cette Recommandation intervient dans la couche application. Les notifications d'alarme de sécurité définies par cette fonction de gestion des systèmes fournissent des informations concernant l'état opérationnel et la qualité de service concernant la sécurité.	CE 4
X.740	Technologie de l'information – Interconnexion de systèmes ouverts – Gestion-systèmes: fonction de piste de vérification de sécurité	Cette Recommandation définit la fonction de piste de vérification de sécurité. Il s'agit d'une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée afin d'échanger les informations et commandes de gestion des systèmes. Cette fonction se situe dans la couche application.	CE 4

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.741	Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: objets et attributs de contrôle d'accès	Cette Recommandation contient des spécifications applicables à la fourniture du contrôle d'accès dans les applications utilisant les services et protocoles de gestion OSI. Les informations de contrôle d'accès figurant dans cette Recommandation pourront être utilisées pour mettre en œuvre des modes de contrôle d'accès fondés sur des listes de contrôle d'accès, sur des capacités, sur des étiquettes de sécurité et sur des contraintes contextuelles.	CE 4
X.790	Fonction de gestion des dérangements pour les applications de l'UIT-T	Cette Recommandation concerne la gestion des dysfonctionnements de systèmes et de réseaux de communication du point de vue du prestataire et de l'usager du service. Un dysfonctionnement, appelé "dérangement" dans cette Recommandation, est un problème influençant d'une manière défavorable la qualité de service telle qu'elle est perçue par les usagers du réseau. Lorsqu'un dérangement est détecté, par exemple à la suite d'un signalement d'alarme, un dossier de dérangement peut être saisi par un usager ou généré automatiquement par le système. Il est nécessaire de gérer ce dossier de dérangement pour garantir qu'il est pris en compte et résolu de manière à rétablir le service à son niveau antérieur. Un format de dossier est défini, qui permet à un usager de signaler un dérangement qui progressera ensuite vers sa résolution, après sa prise en charge par un prestataire. L'usager peut déterminer, pendant la résolution du dérangement par le prestataire de service, l'état actuel de la résolution en émettant une demande concernant cette information. Le fournisseur peut envoyer une notification à l'usager lorsque le dossier de dérangement est résolu. Des types particuliers de dérangement sont définis; toutefois, l'utilisation de cette Recommandation par une application donnée peut nécessiter que des dérangements propres à cette application soient mis en œuvre, ce qui est prévu. Il est possible qu'au moment du dérangement, le réseau était interconnecté avec un autre dans le but de fournir un service et que l'origine du problème ou de la défaillance se situait dans cet autre réseau. Pour cette raison, il peut être utile que les systèmes de gestion échangent des informations sur le traitement des dérangements via des interfaces, qui peuvent se situer entre un client et un prestataire de services ou entre deux prestataires de services. Ces interfaces peuvent représenter des limites entre des domaines de compétence ou à l'intérieur des domaines de compétence. Il peut aussi être utile d'échanger, en plus des informations sur les défaillances constatées, des renseignements préliminaires sur l'indisponibilité du service, pour des raisons de maintenance programmée, par exemple. Le domaine d'application de cette Recommandation englobe tous ces aspects de l'échange d'information.	CE 4
X.800	Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT	Cette Recommandation définit les éléments généraux d'architecture ayant trait à la sécurité, que l'on peut appliquer de façon appropriée dans les cas où une protection de la communication entre systèmes ouverts est requise. Dans le cadre du modèle de référence, elle établit des principes directeurs et des contraintes permettant d'améliorer les Recommandations existantes ou d'élaborer de nouvelles Recommandations dans le contexte de l'OSI pour permettre des communications sûres et donner ainsi une approche cohérente de la sécurité dans l'OSI. Cette Recommandation est une extension du modèle de référence destinée à couvrir les aspects de sécurité qui sont des éléments généraux d'architecture des protocoles de communication, mais qui ne sont pas traités dans le modèle de référence. Cette Recommandation donne une description générale des services de sécurité et des mécanismes associés qui peuvent être fournis par le modèle de référence et signale, dans le modèle de référence, les emplacements où les services et mécanismes peuvent être fournis.	CE 17
X.802	Technologies de l'information – Modèle de sécurité des couches inférieures	Cette Recommandation décrit les aspects intercouches de la fourniture des services de sécurité dans les couches inférieures du Modèle de référence OSI (couches transport, réseau, liaison de données et physique). Elle décrit les concepts architecturaux communs à ces couches, la base des interactions entre couches relatives à la sécurité, et le positionnement des protocoles de sécurité dans les couches inférieures.	CE 17
X.803	Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures	Cette Recommandation décrit la sélection, l'insertion et l'utilisation des services et mécanismes de sécurité dans les couches supérieures (application, présentation et session) du modèle de référence OSI.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.805	Architecture de sécurité pour les systèmes assurant des communi-cations de bout en bout	Cette Recommandation définit les éléments généraux d'architecture ayant trait à la sécurité, qui, lorsqu'ils sont mis en œuvre comme il convient, en particulier dans un environnement multifabricants, garantissent qu'un réseau est correctement protégé contre les attaques malveillantes et contre celles qui se produisent par inadvertance, qu'il présente une grande disponibilité et des délais de réponse appropriés, qu'il est intègre et évolutif et qu'il comporte une fonction de facturation précise.	CE 17
X.810	Technologies de l'infor-mation – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général	Cette Recommandation définit le cadre dans lequel les services de sécurité pour les systèmes ouverts sont spécifiés. Cette partie des cadres de sécurité définit l'organisation du *cadre de sécurité*, définit les *concepts de sécurité* requis dans plusieurs parties des cadres de sécurité, et décrit les interrelations des services et mécanismes identifiés dans les autres parties du cadre. Ce cadre décrit tous les aspects d'*authentification* tels qu'ils s'appliquent aux systèmes ouverts, la relation entre l'authentification et d'autres fonctions de sécurité comme le *contrôle d'accès* et les besoins de gestion pour l'authentification.	CE 17
X.811	Technologies de l'infor-mation – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification	Cette Recommandation définit un cadre général pour la fourniture de l'authentification. L'authentification vise essentiellement à *contrer les menaces d'usurpation d'identité et de réexécution*.	CE 17
X.812	Technologies de l'infor-mation – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès	Cette Recommandation définit un cadre général pour la fourniture du contrôle d'accès. Le but essentiel du contrôle d'accès est de *parer au risque d'opérations non autorisées* au moyen d'un ordinateur ou d'un système de communication; ces menaces sont fréquemment subdivisées en classes qui sont notamment les suivantes: *utilisation non autorisée, divulgation, modification, destruction et déni de service*.	CE 17
X.813	Technologies de l'infor-mation – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: non-répudiation	Cette Recommandation définit un cadre général pour la fourniture d'un service de non-répudiation. Le service de non-répudiation a pour objet *de collecter, de conserver, de diffuser et de valider des preuves irréfutables concernant l'identification des expéditeurs et des destinataires participant à des transferts de données*.	CE 17
X.814	Technologies de l'infor-mation – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité	Cette Recommandation définit un cadre général pour la fourniture de services de confidentialité. La confidentialité est une propriété selon laquelle *aucune information n'est communiquée ou divulguée* à des individus, entités ou processus non autorisés.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.815	Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité	Cette Recommandation définit un cadre général pour la fourniture de services d'intégrité. La propriété caractérisant *des données qui n'ont pas été altérées ou détruites* d'une manière non autorisée est appelée "intégrité".	CE 17
X.816	Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité	Cette Recommandation décrit un modèle de base permettant de manipuler les alarmes de sécurité et de conduire un audit de sécurité pour les systèmes ouverts. Un audit de sécurité est *une analyse et un examen – effectués de façon indépendante – des enregistrements et activités du système*. Le service d'audit de sécurité fournit à une autorité d'audit la capacité de spécifier, sélectionner et gérer les événements qui doivent être enregistrés dans un journal d'audit de sécurité.	CE 17
X.830	Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: aperçu général, modèles et notation	Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle définit: a) *des modèles* généraux *de fonctions de protocole d'échanges de sécurité et des transformations de sécurité*; b) une série d'*outils de notation* pour spécifier les besoins de protection sélective des champs dans une spécification de syntaxe abstraite, les échanges de sécurité et les transformations de sécurité; c) une série de *lignes directrices informatives* sur l'application des moyens de sécurité génériques des couches supérieures traités dans cette série de Recommandations.	CE 17
X.831	Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: définition du service assuré par l'élément de service d'échange de sécurité	Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle spécifie le service fourni par l'élément de service d'échange de sécurité (SESE, *security exchange service element*) qui est un élément de service d'application (ASE) facilitant la communication des informations nécessaires pour assurer les *services de sécurité* dans la couche application de l'OSI.	CE 17
X.832	Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: spécification du protocole d'élément de service d'échange de sécurité	Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle *spécifie le protocole* fourni par l'élément de service d'échange de sécurité (SESE) qui est un élément de service d'application (ASE) facilitant la communication des informations nécessaires pour assurer les *services de sécurité* dans la couche application de l'OSI.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.833	Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: spécification de la syntaxe de protection du transfert	Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle spécifie la syntaxe de protection du transfert qui est utilisée en association avec la couche présentation pour assurer des *services de sécurité* dans la couche application.	CE 17
X.834	Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: formulaire de déclaration de conformité d'instance de protocole de l'élément de service d'échange de sécurité	Cette Recommandation fait partie d'une série de Recommandations sur la sécurité générique des couches supérieures (GULS, *generic upper layers security*). Elle contient le formulaire de déclaration de conformité d'instance de protocole (PICS, *protocol implementation conformance statement*) pour le protocole d'élément de service d'échange de sécurité spécifié dans la Rec. UIT-T X.832 et pour les échanges de sécurité décrits dans la Rec. UIT-T X.830. L'Annexe C décrit les capacités et options normalisées sous une forme qui permet l'évaluation, aux fins de conformité, d'une réalisation donnée.	CE 17
X.835	Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: formulaire de déclaration de conformité d'instance de protocole de la syntaxe de protection de transfert	Cette Recommandation fait partie d'une série de Recommandations sur la sécurité générique des couches supérieures (GULS, *generic upper layers security*). Elle contient le formulaire de déclaration de conformité d'instance de protocole (PICS, *protocol implementation conformance statement*) pour la spécification de la syntaxe de protection du transfert figurant dans la Rec. UIT-T X.833. Cette Recommandation décrit les capacités et options normalisées sous une forme qui permet l'évaluation, aux fins de conformité, d'une réalisation donnée.	CE 17
X.841	Technologies de l'information – Techniques de sécurité – Objets informationnels de sécurité pour le contrôle d'accès	Cette Recommandation rassemble les définitions d'objets courantes utiles pour les *normes de sécurité* afin d'éviter la présence de définitions multiples et différentes de la même fonctionnalité. L'utilisation de la notation de syntaxe abstraite numéro un (ASN.1) a permis d'obtenir des définitions précises. Cette Recommandation ne couvre que les aspects statiques des objets d'information de sécurité (SIO, *security information object*).	CE 17
X.842	Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance	Cette Recommandation traite des services qui ont recours à des tiers de confiance (TTP, *trusted third party*). Elle propose des lignes directrices sur leur utilisation et sur la gestion des services, une définition claire des responsabilités et des services de base, la description et l'objet de ceux-ci, ainsi que les rôles et les responsabilités des TTP et des entités qui font appel à leurs services. Elle distingue les différentes catégories de services TTP, notamment *l'horodatage, la non-répudiation, la gestion de clés, la gestion de certificats et le notaire électronique*.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.843	Technologies de l'information – Techniques de sécurité – Spécification des services de tiers de confiance pour la prise en charge des applications de signature numérique	Cette Recommandation définit les services nécessaires à la prise en charge des applications de signature numérique pour la *non-répudiation* de création d'un document. Comme cette prise en charge suppose que le document est *intègre* et que le créateur est *authentique*, les services décrits peuvent également être couplés aux *services responsables de l'intégrité et de l'authenticité*.	CE 17
X.901	Technologies de l'information – Traitement réparti ouvert – Modèle de référence: aperçu général	La croissance rapide des applications réparties a fait naître le besoin d'un cadre pour coordonner la normalisation du traitement réparti ouvert (ODP, *open distributed processing*). Le modèle de référence ODP fournit ce cadre. Il établit une architecture qui permet la prise en compte de la répartition, de l'interfonctionnement et de la portabilité. Cette Recommandation contient un aperçu général du modèle de référence ODP, en précise les motivations, le domaine d'application et la justification, avec une explication des concepts clés ainsi qu'une présentation de l'architecture ODP. Elle explique la façon d'interpréter ce modèle de référence et la manière dont il peut être utilisé, en particulier par les rédacteurs de normes et par les architectes de systèmes ODP. Elle contient également une classification des domaines de normalisation en matière de systèmes répartis; cette classification s'appuie sur les points de référence de conformité identifiés dans la Rec. UIT-T X.903. Les systèmes ODP doivent être fiables, c'est-à-dire que leur construction et leur maintenance doit être telle que les services offerts par le système et les données qui lui sont confiées soient *protégés contre les accès non autorisés, les utilisations illicites et toute autre menace ou attaque*. Il est plus difficile d'assurer le niveau de sécurité requis dès lors que les interactions ont lieu à distance et que des parties du système et ses utilisateurs sont mobiles. Les règles de sécurité pour les systèmes ODP peuvent définir: *la détection des menaces pesant sur la sécurité*; *la protection contre les menaces pesant sur la sécurité*; *la limitation des dommages causés par toute atteinte à la sécurité*.	CE 17
X.902	Technologies de l'information – Traitement réparti ouvert – Modèle de référence: fondements	Cette Recommandation définit les concepts et le cadre analytique servant à la description normalisée de systèmes (arbitraires) de traitement réparti. Elle introduit les principes de la conformité aux normes de traitement réparti ouvert (ODP) et la manière de les appliquer. Elle s'en tient à un niveau de détail suffisant pour *établir les prescriptions de nouvelles techniques de spécification*.	CE 17
X.903	Technologies de l'information – Traitement réparti ouvert – Modèle de référence: architecture	Cette Recommandation contient la spécification des caractéristiques requises pour qu'un système de traitement réparti puisse être qualifié d'ouvert: il s'agit des contraintes que doivent respecter les normes de traitement réparti ouvert (ODP, *open distributed processing*). Cette Recommandation utilise les techniques descriptives décrites dans la Rec. UIT-T X.902.	CE 17
X.904	Technologies de l'information – Traitement réparti ouvert – Modèle de référence: sémantique architecturale	Cette Recommandation contient une normalisation des concepts de modélisation ODP définis aux § 8 et 9 de la Rec. UIT-T X.902. La normalisation est obtenue par l'interprétation de chaque concept en fonction des constructions des différentes techniques de description formelle normalisées.	CE 17

N°	TITRE	OBJET PRINCIPAL ET ASPECTS LIÉS À LA SÉCURITÉ	Commission d'études
X.1051	Système de gestion de la sécurité de l'information – Prescriptions pour les télécommunications (ISMS-T)	Pour les organisations de télécommunication, l'information et les processus qui permettent de la traiter, les installations de télécommunication, les réseaux et les lignes sont des biens essentiels à leur activité. Pour que les organisations de télécommunication puissent gérer de manière adéquate ces biens et poursuivre avec succès leur activité, il leur est absolument nécessaire d'avoir une bonne maîtrise de la sécurité de l'information. Elle énonce les prescriptions relatives à la gestion de la sécurité de l'information pour les organisations de télécommunication. Elle expose les conditions de mise en place, d'implémentation, d'exploitation, de supervision, de réexamen, de maintenance et d'amélioration d'un système ISMS documenté dans le contexte des risques globaux afférents aux télécommunications. Elle expose également les conditions d'implémentation de contrôles de sécurité adaptés aux besoins spécifiques de chaque organisation de télécommunication ou de certaines parties d'entre elles.	CE 17
X.1081	Le modèle télébiométrique multimodal – Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie	Cette Recommandation définit un modèle télébiométrique multimodal qui constitue un cadre général commun pour la spécification de quatre aspects interdépendants de la sécurité: secret, authentification, innocuité et sécurité. Le modèle couvre toutes les possibilités sécurisées et sans danger d'interactions multimodales homme-machine; il s'appuie en partie sur les normes ISO 31 et CEI 60027-1. Les modalités d'interactions cognitives, sensorielles et comportementales d'un individu sont également à prendre en compte dans le cadre des télécommunications et sont susceptibles d'être utilisées à l'avenir par un capteur ou un effecteur biométrique à des fins d'authentification; aussi sont-elles également intégrées au modèle. Le modèle propose une typologie des interactions susceptibles de se produire au niveau de la couche multimodale correspondant au contact de l'organisme humain avec différents dispositifs électroniques, photoniques, chimiques ou matériels, qui saisissent des paramètres biométriques ou qui ont une incidence sur cet organisme; l'authentification d'un être humain, de manière à préserver sa sécurité et son intimité, peut être spécifiée en termes d'interactions entre ces dispositifs et la sphère privée personnelle; par ailleurs, la modélisation et le regroupement des interactions d'un individu avec son environnement permettent d'expliciter et de structurer leur analyse. Cette Recommandation contient une spécification de la sphère privée individuelle, de la classification des modalités d'interaction impliquant cette sphère, des unités de base et des unités dérivées pour la mesure et la spécification (quantitatives) des interactions et d'une échelle de proximité relative.	CE 17
X.1121	Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout	Cette Recommandation décrit les problèmes de sécurité qui se posent dans le contexte des communications de données de bout en bout, ainsi que les besoins de sécurité du point de vue de l'utilisateur mobile et du fournisseur de services d'application dans la couche supérieure du modèle de référence OSI, pour les communications mobiles de données de bout en bout entre un terminal mobile de réseau mobile et un serveur d'application de réseau ouvert. Par ailleurs, elle indique les points d'intervention, dans les modèles de communications mobiles de données de bout en bout, des techniques de sécurité qui entrent en jeu dans certaines fonctions de sécurité. Elle définit un cadre général de technologies de sécurité pour les communications mobiles de données de bout en bout.	CE 17
X.1122	Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI)	Les technologies de sécurité fondées sur l'infrastructure de clés publiques sont appliquées à la relation entre terminaux mobiles et serveurs d'application dans le modèle général des systèmes mobiles de communication de données de bout en bout entre utilisateurs mobiles et fournisseurs de services d'application ou à la relation entre terminaux mobiles et passerelle de sécurité mobile d'une part et entre passerelle de sécurité mobile et serveur dans le modèle avec passerelle des communications mobiles de données de bout en bout entre utilisateurs mobiles et fournisseurs de services d'application. Bien qu'elles constituent des technologies propres à mettre en œuvre de nombreuses fonctions de sécurité (chiffrement, signature numérique, intégrité des données, etc.) dans le cadre des communications mobiles de données de bout en bout, les technologies à infrastructure de clés publiques (PKI) doivent être adaptées à ce type d'utilisation. Les méthodes permettant de construire et de gérer des systèmes mobiles sécurisés fondés sur les technologies PKI n'ayant pas encore été définies, cette Recommandation décrit le cadre général pour l'établissement de systèmes de ce type.	CE 17

Annexe B

Terminologie dans le domaine de la sécurité

Les définitions et abréviations suivantes de l'UIT-T relatives à la sécurité sont extraites de Recommandations de l'UIT-T.

La base de données en ligne de l'UIT-T SANCHO (*Sector Abbreviations and defiNitions for a teleCommunications tHesaurus Oriented*) donne accès aux "termes et définitions" ou aux "abréviations et acronymes" contenus dans les publications de l'UIT-T, en anglais, français et espagnol. Elle est accessible en ligne gratuitement à l'adresse www.itu.int/sancho. Une version CD-ROM est également publiée régulièrement. SANCHO contient l'ensemble des termes et des définitions figurant dans la présente Annexe, accompagnés de la liste des Recommandations où le terme ou la définition est utilisé.

La CE 17 de l'UIT-T a élaboré un recueil de définitions relatives à la sécurité utilisées dans les Recommandations de l'UIT-T, accessible à l'adresse
www.itu.int/ITU-T/studygroups/com17/tel-security.html

B.1 Liste de termes et définitions relatifs à la sécurité

La liste suivante contient les termes relatifs à la sécurité les plus couramment utilisés qui sont définis dans les Recommandations de l'UIT-T en vigueur. Le recueil tenu à jour par la Commission d'études 17 (voir le lien donné plus haut) contient une liste plus complète de définitions relatives à la sécurité.

Terme	Définition	Référence
Contrôle d'accès (*access control*)	1. Précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée. 2. Restriction du flux d'informations provenant des ressources d'un système aux personnes, programmes, processus ou autres ressources de système de réseau autorisés.	X.800 J.170
Liste de contrôle d'accès (*access control list*)	Liste des entités qui sont autorisées à accéder à une ressource, avec leurs autorisations d'accès.	X.800
Politique de contrôle d'accès (*access control policy*)	Ensemble des règles définissant les conditions dans lesquelles l'accès peut se dérouler.	X.812
Service de contrôle d'accès (*access control service*)	Le service de contrôle d'accès fournit le moyen de garantir que l'accès à des ressources par les acteurs se fait uniquement de manière autorisée. Les ressources en question peuvent être le système physique, le logiciel système, les applications et les données. Le service de contrôle d'accès peut être défini et implémenté dans le RGT au niveau agent, au niveau objet ou au niveau attribut. Les limitations d'accès sont indiquées dans les informations de contrôle d'accès qui spécifient: les moyens permettant de déterminer quelles sont les entités qui disposent d'une autorisation d'accès; le type d'accès autorisé (lecture, écriture, modification, création, suppression).	M.3016.2
Menaces accidentelles (*accidental threats*)	Menaces qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles qui se sont concrétisées sont: défaillance de système, bévues opérationnelles et bogues dans le logiciel.	X.800
Imputabilité (*accountability*)	Propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité.	X.800
Menace active (*active threat*)	Menace de modification non autorisée et délibérée d'informations contenues dans le système ou modification de l'état du système. *Note* – La modification et la répétition de messages, l'insertion de faux messages, l'usurpation de l'identité d'une entité autorisée, le déni de service et la modification malveillante des tables de routage d'un système par un utilisateur non autorisé sont des exemples de menaces actives.	X.800
Arbitre (*adjudicator*)	Entité qui règle les litiges qui peuvent apparaître à la suite d'événements ou d'actions répudiés, c'est-à-dire qui évalue les preuves et détermine si l'action ou l'événement litigieux a eu lieu. L'arbitrage ne peut être assuré efficacement que si les parties au litige acceptent l'autorité de l'arbitre.	X.813
Algorithme (*algorithm*)	Processus mathématique qui peut être utilisé pour l'embrouillage et pour le désembrouillage d'un flux de données.	J.93
Méthode d'authentification asymétrique (*asymmetric authentication method*)	Méthode d'authentification dans laquelle toutes les informations d'authentification ne sont pas partagées par les deux entités.	X.811

Terme	Définition	Référence
Algorithme asymétrique de cryptographie (*asymmetric cryptographic algorithm*)	Algorithme pour réaliser le chiffrement ou le déchiffrement correspondant dans lequel les clés utilisées pour le chiffrement et le déchiffrement sont différentes. *Note* – Avec certains algorithmes asymétriques de cryptographie, il faut utiliser plus d'une clé privée pour déchiffrer un cryptogramme ou pour générer une signature numérique.	X.810
Attaque (*attack*)	Activités entreprises pour contourner ou exploiter des déficiences constatées dans les mécanismes de sécurité d'un système. Une attaque directe d'un système exploite des déficiences dans les algorithmes, principes ou propriétés sous-tendant un mécanisme de sécurité. Les attaques indirectes consistent à contourner le mécanisme ou à en provoquer une utilisation incorrecte par le système.	H.235
Attribut (*attribute*)	Dans le cadre de la messagerie, élément d'information, composante d'une liste d'attributs, qui décrit un utilisateur ou une liste de distribution et qui peut aussi se rapporter à la structure physique ou organisationnelle du système de messagerie (ou du réseau qui le supporte).	X.400
Autorité d'attribut, autorité en charge des attributs (*attribute authority*)	1. Autorité qui attribue des privilèges par l'émission de certificats d'attribut. 2. Entité bénéficiant de la confiance d'une ou de plusieurs entités pour l'établissement et la signature de certificats d'attribut. *Note* – Une autorité de certification peut également être une autorité en charge des attributs.	X.509 X.842
Certificat d'attribut (*attribute certificate*)	Structure de données, portant la signature numérique d'une autorité d'attribut, qui lie certaines valeurs d'attribut à des informations d'identification concernant son détenteur.	X.509
Type d'attribut (*attribute type*)	Identificateur qui désigne une classe d'information (par exemple: nom personnel). Il s'agit d'une partie d'un attribut.	X.400
Valeur d'attribut (*attribute value*)	Elément de la classe d'information qu'un type d'attribut désigne (par exemple: un nom personnel particulier). Il s'agit d'une partie d'un attribut.	X.400
Audit	Voir audit de sécurité (*security audit*).	X.400
Journal d'audit (*audit trail*)	Voir journal d'audit de sécurité (*security audit trail*).	X.800
Identité authentifiée (*authenticated identity*)	Identificateur distinctif d'entité principale qui a été attesté par une authentification.	X.811
Authentification (*authentication*)	1. Processus de confirmation d'identité. *Note* – Voir entité principale (*principal*) et vérificateur (*verifier*) et les deux formes d'authentification distinguées (auth. de l'origine des données (*data origin auth.*) + auth. d'identité (*entity auth.*)). L'authentification peut être *unilatérale* ou *mutuelle*. La première atteste l'identité d'une seule entité principale. La seconde atteste l'identité des deux entités principales. 2. Attestation de l'identité revendiquée par une entité. 3. Voir authentification de l'origine des données (*data origin authentication*) et authentification de l'entité homologue (*peer entity authentication*). Le terme authentification n'est pas associé à l'intégrité des données; le terme intégrité des données est utilisé à la place. 4. Corroboration de l'identité des objets se rapportant à l'établissement d'une association. Par exemple, il peut s'agir des entités d'application, des processus d'application et des usagers des applications. *Note* – Ce terme a été défini en vue d'indiquer clairement qu'il s'agit d'une authentification de portée plus large que l'authentification de l'entité homologue dont traite la Rec. X.800 du CCITT. 5. Processus consistant à vérifier l'identité déclarée d'une entité auprès d'une autre entité. 6. Processus destiné à permettre au système de vérifier avec certitude l'identité d'un tiers.	X.811 X.811 X.800 X.217 J.170 J.93

Terme	Définition	Référence
Certificat d'authentification (*authentication certificate*)	Certificat de sécurité qui est garanti par une autorité d'authentification et qui peut être utilisé pour attester l'identité d'une entité.	X.811
Echange d'authentification, échange pour authentification (*authentication exchange*)	1. Mécanisme destiné à garantir l'identité d'une entité par échange d'informations. 2. Séquence d'un ou de plusieurs transferts d'informations d'authentification (AI) pour échange, en vue de réaliser une authentification.	X.800 X.811
Service d'authentification (*authentication service*)	Ce service fournit la preuve qu'un objet ou un sujet possède effectivement l'identité qu'il déclare. Les types d'authentification suivants peuvent être nécessaires en fonction du type d'acteur et du but de l'identification: authentification de l'utilisateur, authentification de l'entité homologue, authentification de l'origine des données. Des exemples de mécanismes utilisés pour implémenter le service d'authentification sont l'authentification simple par mot de passe et numéro d'identification personnel (PIN, *personal identification number*) et l'authentification forte basée sur des méthodes de chiffrement.	M.3016.2
Jeton d'authentification, jeton (*authentication token; token*)	Information véhiculée pendant un échange d'authentification forte et pouvant être utilisée pour authentifier son émetteur.	X.509
Authenticité (*authenticity*)	1. Capacité de garantir que l'information donnée n'a été ni modifiée ni falsifiée et qu'elle a bien été produite par l'entité qui déclare l'avoir fournie. 2. Propriété consistant à pouvoir vérifier la source déclarée des données à la satisfaction du destinataire.	J.170 T.411
Autorité (*authority*)	Entité responsable de l'émission de certificats. Deux types sont définis: les autorités de certification émettant des certificats de clé publique et les autorités d'attribut émettant des certificats d'attribut.	X.509
Certificat d'autorité (*authority certificate*)	Certificat émis à destination d'une autorité (par exemple, une autorité de certification ou une autorité d'attribut).	X.509
Autorisation (*authorization*)	1. Attribution de droits, comprenant la permission d'accès sur la base de droits d'accès. *Note* – Cette définition implique que les droits sont des droits d'effectuer certaines activités (telles que l'accès aux données) et qu'ils ont été accordés à une entité, un opérateur humain ou un processus. 2. Octroi d'une permission sur la base d'une identité authentifiée. 3. Fait de donner l'accès à un service ou à un dispositif à quelqu'un qui dispose de la permission d'accès.	X.800 H.235 J.170
Disponibilité (*availability*)	Propriété d'être accessible et utilisable sur demande par une entité autorisée.	X.800
Portail de sécurité de câble (CSP, *cable security portal*)	Elément fonctionnel qui fournit des fonctions de gestion de la sécurité et de conversion entre l'hybride HFC et l'utilisateur résidentiel.	J.191
Serveur de gestion d'appel (CMS, *call management server*)	IPCablecom. Serveur qui contrôle les connexions audio, également appelé agent d'appel dans la terminologie du protocole MGCP/SGCP.	J.191
Capacité (*capability*)	Jeton utilisé comme identificateur d'une ressource de telle sorte que la possession du jeton confère des droits d'accès à cette ressource.	X.800
Certificat (*certificate*)	Ensemble de données relatives à la sécurité, émis par une autorité de sécurité ou par un tiers de confiance en même temps que des informations de sécurité qui sont utilisées pour fournir les services d'intégrité et d'authentification d'origine des données (certificat de sécurité – X.810). Ce terme vise des certificats "à clé publique" qui sont des valeurs représentant une clé publique de détenteur (et d'autres informations facultatives), ces valeurs ayant été vérifiées et signées par une autorité de confiance sous une forme infalsifiable.	H.235

Terme	Définition	Référence
Politique de certificat (*certificate policy*)	Ensemble nommé de règles indiquant la possibilité d'appliquer un certificat pour une communauté particulière et/ou une classe d'applications particulière avec des besoins de sécurité communs. Une politique de certificat particulière peut, par exemple, indiquer la possibilité d'application d'un certificat pour des transactions avec échange de données électroniques pour le commerce de biens dans une fourchette de prix donnée.	X.509
Liste de révocation de certificats (CRL, *certificate revocation list*)	1. Liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par leur émetteur. Certains types de listes CRL spécifiques sont définis en plus du type générique de liste CRL, pour couvrir des domaines particuliers. 2. Une liste CRL contient les numéros de série des certificats qui ont été révoqués (par exemple parce que la clé a été compromise ou parce que le sujet ne fait plus partie du personnel) et dont la période de validité n'a pas encore expiré.	X.509 Q.817
Autorité de certification (CA, *certification authority*)	1. Autorité jouissant de la confiance d'un ou de plusieurs utilisateurs pour la création et l'attribution de certificats. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs. 2. Entité habilitée à laquelle il est fait confiance (dans le contexte d'une politique de sécurité) pour créer des certificats de sécurité contenant une ou plusieurs classes de données relatives à la sécurité.	X.509 X.810
Itinéraire de certification (*certification path*)	Séquence ordonnée de certificats concernant des objets contenus dans l'arbre DIT et qui peuvent être traités à partir de la clé publique de l'objet initial de l'itinéraire pour obtenir l'objet final de cet itinéraire.	X.509
Epreuve (*challenge*)	Paramètre variable dans le temps produit par un vérificateur.	X.811
Chiffre (*cipher*)	1. Algorithme cryptographique ou transformée mathématique. 2. Algorithme qui convertit un texte en clair en texte chiffré.	H.235 J.170
Cryptogramme, texte chiffré (*ciphertext*)	Données obtenues par l'utilisation du chiffrement. Le contenu sémantique des données résultantes n'est pas compréhensible. NOTE – Le cryptogramme peut lui-même être réinjecté dans un nouveau chiffrement pour produire un cryptogramme surchiffré.	X.800
Déclarant (*claimant*)	Entité qui est ou représente une *entité principale* à des fins d'authentification. Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.	X.811
Texte en clair (*cleartext*)	Données intelligibles dont la sémantique est compréhensible.	X.800
Preuve compromise (*compromised evidence*)	Preuve, qui avait été satisfaisante à un moment donné, mais en laquelle le tiers de confiance ou l'arbitre n'a plus confiance.	X.813
Confidentialité (*confidentiality*)	Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.	X.800
Service de confidentialité (*confidentiality service*)	Le service de confidentialité fournit une protection contre la divulgation non autorisée de données échangées. On peut distinguer les types de service de confidentialité suivants: confidentialité sélective de champ, confidentialité en mode connexion, confidentialité de flux de données.	M.3016.2
Intégrité du contenu (*content integrity*)	1. Permet au destinataire de vérifier que le contenu original d'un message n'a pas été modifié. 2. Cet élément de service permet à l'émetteur d'un message de fournir au récepteur un moyen permettant à ce dernier de vérifier que le contenu du message n'a pas été modifié. L'intégrité du contenu est valable message par message et peut mettre en œuvre un procédé de chiffrement asymétrique ou symétrique.	X.400 X.400

Terme	Définition	Référence
Contresignature (*counter-signature*)	Signature numérique ajoutée à une unité de données déjà signée par une entité différente (par exemple un tiers habilité).	X.813
Justificatif d'identité (*credentials*)	Données transférées pour établir l'identité déclarée d'une entité.	X.800
Analyse cryptographique (*cryptanalysis*)	1. Analyse d'un système cryptographique, et/ou de ses entrées et sorties, pour en déduire des variables confidentielles et/ou des données sensibles (y compris un texte en clair). 2. Processus consistant à récupérer le texte en clair d'un message ou la clé de chiffrement sans avoir accès à la clé. 3. Science de la récupération du contenu d'un message sans accéder à la clé physique (ou à la clé électronique dans un système cryptographique électronique).	X.800 J.170 J.93
Algorithme cryptographique (*cryptographic algorithm*)	Fonction mathématique qui calcule un résultat à partir d'une ou de plusieurs valeurs d'entrée.	H.235
Chaînage cryptographique (*cryptographic chaining*)	Mode d'utilisation d'un algorithme cryptographique dans lequel la transformation effectuée par l'algorithme dépend des valeurs des entrées ou sorties précédentes.	X.810
Valeur de contrôle cryptographique (*cryptographic checkvalue*)	Information obtenue en réalisant une transformation cryptographique (voir cryptographie (cryptography)) sur une unité de données. *Note* – La valeur de contrôle peut être obtenue en une ou plusieurs étapes et résulte d'une fonction mathématique utilisant la clé et une unité de données. Elle permet de vérifier l'intégrité d'une unité de données.	X.800
Système de chiffrement (*cryptographic system, cryptosystem*)	1. Ensemble de transformations d'un texte en clair pour obtenir un texte chiffré et réciproquement, le choix de la ou des transformations particulières à utiliser se faisant au moyen de clés. Les transformations sont définies en général par un algorithme mathématique. 2. Un système de chiffrement est simplement un algorithme qui peut convertir des données d'entrée en quelque chose de non reconnaissable (chiffrement), et reconvertir ces données non reconnaissables dans leur forme d'origine (déchiffrement). Les techniques de chiffrement RSA sont décrites dans la Rec. UIT-T X.509.	X.509 Q.815
Cryptographie (*cryptography*)	Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée. *Note* – La cryptographie détermine les méthodes de chiffrement et de déchiffrement. Une attaque portant sur les principes, moyens et méthodes de cryptographie est appelée analyse cryptographique.	X.800
Confidentialité des données (*data confidentiality*)	Ce service peut être utilisé pour protéger des données contre une divulgation non autorisée. Le service de confidentialité des données est pris en charge par le cadre d'authentification. Il peut être utilisé pour protéger des données contre les interceptions.	X.509
Intégrité des données (*data integrity*)	Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.	X.800
Authentification de l'origine des données (*data origin authentication*)	1. Confirmation que la source des données reçues est telle que déclarée. 2. Corroboration de l'identité de l'entité principale qui est responsable d'une unité de données spécifique.	X.800 X.811
Déchiffrement (*decipherment, decryption*)	Opération inverse d'un chiffrement réversible.	X.800
Délégation (*delegation*)	Transfert d'un privilège d'une entité détentrice vers une autre entité.	X.509
Déni de service (*denial of service*)	Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.	X.800

Terme	Définition	Référence
Désembrouillage, déchiffrement (*descrambling*)	1. Restauration des caractéristiques d'un signal image/son/données afin de permettre la réception de l'information en clair. Cette restauration est un processus bien défini, commandé par le système à accès conditionnel (côté réception). 2. Processus inverse de la fonction de chiffrement (voir ce terme) afin d'obtenir des services d'images, de son et de données utilisables.	J.96 J.93
Empreinte numérique (*digital fingerprint*)	Caractéristique d'un élément de données, telle qu'une valeur de contrôle cryptographique ou le résultat de la réalisation d'une fonction de hachage unidirectionnelle sur les données, qui est suffisamment spécifique à l'élément de données pour qu'il ne soit pas possible de trouver, de façon informatique, un autre élément de données ayant les mêmes caractéristiques.	X.810
Signature numérique (*digital signature*)	1. Données ajoutées à une unité de données, ou transformation cryptographique (voir cryptographie (*cryptography*)) d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la falsification (par le destinataire, par exemple). 2. Transformation cryptographique d'une unité de données qui permet au destinataire de l'unité de données de prouver l'origine et l'intégrité de cette unité de données, qui protège l'émetteur et le destinateur de l'unité de données contre un faux fabriqué par un tiers et qui protège l'émetteur contre un faux fabriqué par le destinataire.	X.800 X.843
Attaque directe (*direct attack*)	Attaque d'un système fondé sur les déficiences des algorithmes, des principes ou des propriétés sur lesquels s'appuie un mécanisme de sécurité.	X.814
Service d'annuaire (*directory service*)	Service pour la recherche et la récupération d'informations à partir d'un catalogue d'objets bien définis, qui peut contenir des informations sur les certificats, numéros de téléphone, conditions d'accès, adresses, etc. Un exemple en est un service d'annuaire conforme à la Rec. UIT-T X.500.	X.843
Technique de double enveloppe (*double enveloping technique*)	Une protection supplémentaire peut être assurée à un message complet, y compris à ses paramètres d'enveloppe, grâce à la possibilité de spécifier que le contenu d'un message constitue lui-même un message complet, c'est-à-dire en utilisant une technique de double enveloppe, qui utilise l'argument Type de contenu qui permet de spécifier que le contenu d'un message est une Enveloppe intérieure.	X.402
Ecoutes (indiscrètes) (*eavesdropping*)	Violation de la confidentialité par surveillance de la communication.	M.3016.0
Clé électronique (*electronic key*)	Signaux de données utilisés pour commander le processus de déchiffrement dans les décodeurs d'abonnés. NOTE – Il existe au moins trois types de clés électroniques: celles qui sont utilisées pour les flux de signaux de télévision; celles qui sont utilisées pour protéger les opérations des systèmes de contrôle d'accès; et celles qui sont utilisées pour la distribution de clés électroniques sur le système câblé.	J.93
Chiffrement (*encipherment*)	1. Transformation cryptographique (voir cryptographie (*cryptography*)) de données produisant un cryptogramme. NOTE – Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué. 2. Processus consistant à rendre des données illisibles par des entités non autorisées après application d'un algorithme crypto-graphique (ou de chiffrement). Le déchiffrement est l'opération inverse par laquelle le texte chiffré est transformé en texte clair.	X.800 H.235
Cryptage (*encryption*)	1. Méthode utilisée pour convertir des informations en clair en cryptogramme. 1. Processus de chiffrement des signaux afin d'éviter un accès non autorisé.	J.170 J.93
Entité finale (*end entity*)	Sujet d'un certificat qui utilise sa clé privée à d'autres fins que la signature de certificats ou entité qui est un participant faisant confiance.	X.509

Terme	Définition	Référence
Chiffrement de bout en bout (*end-to-end encipherment*)	Chiffrement de données à l'intérieur ou au niveau du système d'extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système d'extrémité de destination (voir aussi chiffrement liaison par liaison (*link-by-link encipherment*)).	X.800
Entité (*entity*)	1. Un être humain, une organisation, une composante de matériel ou un élément de logiciel. 2. Tout élément concret ou abstrait, qui présente un intérêt. Alors que d'une manière générale le terme entité peut être utilisé pour faire référence à toute chose, son utilisation dans le contexte de la modélisation est réservée aux éléments modélisant l'univers du discours.	X.842 X.902
Authentification d'entité (*entity authentication*)	Corroboration de l'identité d'une entité principale, dans le contexte d'une relation de communication. Note – L'identité authentifiée de cette entité principale n'est garantie que lorsque ce service est invoqué. On peut obtenir la garantie de la continuité d'authentification en suivant la description du 5.2.7/X.811.	X.811
Filtre d'événement (*event discriminator*)	Fonction qui fournit une analyse initiale des événements liés à la sécurité et génère un message d'audit de sécurité et/ou un message d'alarme.	X.816
Preuve (*evidence*)	Information qui, par elle-même ou par association avec d'autres informations, peut être utilisée pour résoudre un litige. *Note* – Formes particulières de preuve: signatures numériques, enveloppes sécurisées et jetons de sécurité. Les signatures numériques sont utilisées avec les techniques de clé publique tandis que les enveloppes sécurisées et les jetons de sécurité sont utilisés avec les techniques de clé privée.	X.813
Générateur de preuve (*evidence generator*)	Entité qui produit une preuve de non-répudiation. *Note* – Cette entité peut être le demandeur du service de non-répudiation, l'expéditeur, le destinataire ou des parties multiples travaillant de concert (par exemple un signataire et un cosignataire).	X.813
Falsification (*forgery*)	Une entité crée de toutes pièces des informations dont elle prétend qu'elles ont été reçues d'une autre entité ou émises à destination d'une autre entité.	M.3016.0
Fonction de hachage (*hash function*)	Fonction (mathématique) qui fait correspondre les valeurs d'un grand ensemble (potentiellement très grand) de valeurs à une gamme plus réduite de valeurs.	X.810
Dissimulation (*hide*)	Opération qui applique une protection par confidentialité à des données non protégées ou une protection par confidentialité supplémentaire à des données déjà protégées.	X.814
Politique de sécurité fondée sur l'identité (*identity-based security policy*)	Politique de sécurité fondée sur les identités et/ou les attributs des utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs et sur les identités et/ou attributs des ressources/objets auxquels on doit accéder.	X.800
Attaque indirecte (*indirect attack*)	Attaque d'un système qui n'est pas fondé sur les déficiences d'un mécanisme de sécurité particulier (par exemple, attaques qui contournent le mécanisme ou qui dépendent de l'utilisation incorrecte du mécanisme par le système).	X.814
Intégrité (*integrity*)	Caractéristique de données qui n'ont pas été altérées de façon non autorisée. (Voir aussi intégrité des données (*data integrity*).)	H.235
Service d'intégrité (*integrity service*)	Le service d'intégrité fournit des moyens permettant d'assurer que les données échangées sont correctes en fournissant une protection contre la modification, la suppression, la création (insertion) et la répétition des données échangées. On peut distinguer les types de service d'intégrité suivants: intégrité sélective de champ; intégrité de connexion sans reprise; intégrité de connexion avec reprise.	M.3016.2
Voie protégée par l'intégrité (*integrity-protected channel*)	Voie de communication à laquelle un service d'intégrité a été appliqué. (Voir intégrité en mode connexion et intégrité en mode sans connexion.)	X.815

Terme	Définition	Référence
Données protégées par l'intégrité (*integrity-protected data*)	Données et tous attributs pertinents se trouvant dans un environnement protégé par l'intégrité.	X.815
Environnement protégé par l'intégrité (*integrity-protected environment*)	Environnement dans lequel toute modification (y compris la création et la suppression) non autorisée de données est empêchée ou est détectable.	X.815
Menaces intentionnelles (*intentional threats*)	Menaces pouvant aller de l'examen fortuit, utilisant des outils de contrôle facilement disponibles, aux attaques sophistiquées, utilisant une connaissance spéciale du système. Une menace intentionnelle qui se concrétise peut être considérée comme une "attaque".	X.800
Résistance à l'intrusion (*intrusion resistance*)	Capacité d'un objet matériel à refuser l'accès physique, électrique ou électromagnétique d'un tiers non habilité à une fonctionnalité interne.	J.93
IPCablecom	Projet UIT-T comprenant une architecture et une série de Recommandations permettant la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems.	J.160
Kerberos	Protocole d'authentification de réseau à clé secrète qui utilise plusieurs algorithmes cryptographiques pour le chiffrement et une base de données de clés centralisée pour l'authentification.	J.170
Clé (key)	1. Série de symboles commandant les opérations de chiffrement et de déchiffrement. 2. Valeur mathématique introduite dans l'algorithme cryptographique choisi.	X.800 J.170
Service de distribution de clés (*key distribution service*)	Service de distribution de clés en toute sécurité à des entités autorisées, fourni par un Centre de distribution de clés et décrit dans l'ISO/CEI 11770-1.	X.843
Echange de clés (*key exchange*)	Echange de clés publiques entre entités à utiliser pour le chiffrement des communications entre ces entités.	J.170
Gestion de clés (*key management*)	Production, stockage, distribution, suppression, archivage et application de clés conformément à une politique de sécurité.	X.800
Fuite d'informations (*leakage of information*)	Lorsque des informations sont acquises par un correspondant non autorisé par surveillance des émissions, par accès non autorisé aux informations stockées dans une entité du système MHS ou par usurpation d'identité, par suite d'une usurpation d'identité et d'un usage abusif du système MTS ou en provoquant un fonctionnement incorrect d'un agent MTA. Les risques de fuite d'informations sont les suivants: perte de confidentialité, perte d'anonymat, détournement de messages, analyse du trafic.	X.402
Chiffrement liaison par liaison (*link-by-link encipherment*)	Application particulière du chiffrement à chaque liaison d'un système de communication (voir aussi chiffrement de bout en bout (*end-to-end encipherment*)). Note – Le chiffrement liaison par liaison implique que les données soient du texte en clair dans les entités relais.	X.800
Perte ou altération des informations (*loss or corruption of information*)	L'intégrité des données transférées est compromise par une action non autorisée de suppression, d'insertion, de modification, de changement d'ordre, de répétition ou de création de retard.	M.3016.0
Détection de modification (*manipulation detection*)	Mécanisme utilisé pour détecter les modifications, accidentelles ou intentionnelles, d'une unité de données.	X.800
Usurpation d'identité (*masquerade*)	Prétention qu'a une entité d'en être une autre.	X.800
Code d'authentification de message (MAC, *message authentication code*)	Valeur de contrôle cryptographique utilisée pour assurer l'intégrité des données et l'authentification de leur origine.	X.813

Terme	Définition	Référence
Authentification de l'origine du message (*message origin authentication*)	Permet au destinataire ou à un MTA quelconque par lequel transite le message, de contrôler l'identité de son expéditeur.	X.400
Intégrité de la séquence des messages (*message sequence integrity*)	1. Permet à l'expéditeur de fournir au destinataire une preuve que la séquence des messages a été respectée. 2. Cet élément de service permet à l'expéditeur d'un message de fournir au destinataire du message un moyen de vérifier que la séquence des messages a été préservée (sans perte de messages, réarrangement ou retransmission) entre l'expéditeur et le destinataire. L'intégrité de la séquence des messages est demandée destinataire par destinataire et peut utiliser des procédés de chiffrement asymétrique ou symétrique.	X.400
Mise en séquence d'un message (*message sequencing*)	Quand une partie ou la totalité d'un message est répétée, différée ou remise en ordre, par exemple pour exploiter l'information d'authentification d'un message correct et remettre en séquence ou différer des messages corrects. Bien que les services de sécurité du système MHS ne permettent absolument pas d'éviter le risque de réexécution, on peut déceler ce risque et en éliminer les effets. Les risques de mise en séquence d'un message comprennent la réexécution de messages, le réarrangement de messages, l'exécution anticipée de messages et le retard de messages.	X.402
Rôle de surveillant (*monitoring role*)	Rôle dans lequel un tiers de confiance contrôle l'action ou l'événement et est censé donner la preuve de ce qui a été surveillé.	X.813
Authentification mutuelle (*mutual authentication*)	Attestation de l'identité des deux entités principales.	X.811
Non-répudiation (*non-repudiation*)	1. Capacité d'empêcher à un émetteur de nier ultérieurement avoir envoyé un message ou exécuté une action. 2. Protection contre le déni, par une des entités impliquées dans une communication, d'avoir participé à tout ou partie de celle-ci. 3. Processus par lequel l'expéditeur d'un message (par exemple une demande de paiement à la séance) ne peut pas nier avoir envoyé ce message.	J.170 H.235 J.93
Notarisation (*notarization*)	Enregistrement de données chez un tiers de confiance permettant de s'assurer ultérieurement de leur exactitude (contenu, origine, date, remise).	X.800
Notaire (*notary*)	Tiers de confiance chez qui les données sont enregistrées afin de pouvoir garantir plus tard l'exactitude des caractéristiques de ces données.	X.813
Menace passive (*passive threat*)	Menace d'une divulgation non autorisée des informations, sans que l'état du système ne soit modifié.	X.800
Mot de passe (*password*)	1. Information d'authentification confidentielle, habituellement composée d'une chaîne de caractères. 2. Chaîne de mot de passe saisie par l'utilisateur: il s'agit de la clé de sécurité attribuée que l'utilisateur mobile partage avec son domaine de rattachement. Ce mot de passe de l'utilisateur et le secret partagé de l'utilisateur qui en découle doivent être utilisés aux fins d'authentification de l'utilisateur.	X.800 H.530
Authentification de l'entité homologue (*peer-entity authentication*)	1. Confirmation qu'une entité homologue d'une association est bien l'entité déclarée. 2. Fourniture de la preuve de l'identité d'une entité homologue durant une relation de communication.	X.800 M.3016.0
Environnement de sécurité personnelle (PSE, *personal security environment*)	Stockage local sûr pour la clé privée d'une entité, pour la clé d'une autorité CA de confiance directe et pour d'autres données éventuelles. En fonction de la politique de sécurité appliquée par l'entité ou en fonction des prescriptions du système, il peut s'agir par exemple d'un fichier protégé par chiffrement ou d'un jeton de matériel inviolable.	X.843

Terme	Définition	Référence
Sécurité physique (*physical security*)	Mesures prises pour assurer la protection des ressources contre des menaces délibérées ou accidentelles.	X.800
Entité principale (*principal*)	Entité dont l'identité peut être authentifiée.	X.811
Respect de la vie privée, secret des communications (*privacy*)	1. Droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées. *Note* – Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité. 2. Mode de communication dans lequel seules les parties explicitement habilitées peuvent interpréter la communication. Le secret des communications est normalement réalisé par chiffrement et par partage de clé(s) pour accéder au chiffre.	X.800 H.235
Clé privée; clé secrète (déconseillé) (*private key; secret key*)	1. (Dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue uniquement par l'utilisateur concerné. 2. Clé qui est utilisée avec un algorithme asymétrique de cryptographie et dont la possession est limitée (habituellement à une seule entité). 3. Clé utilisée en cryptographie à clé publique qui appartient à une entité individuelle et qui doit être tenue secrète.	X.509 X.810 J.170
Privilège (*privilege*)	Attribut ou propriété attribué par une autorité à un utilisateur.	X.509
Infrastructure de gestion de privilège (PMI, *privilege management infrastructure*)	Infrastructure qui peut prendre en charge la gestion des privilèges correspondant à un service complet d'autorisation et en relation avec une infrastructure de clé publique.	X.509
Clé publique (*public key*)	1. (Dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue de manière publique. 2. Clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique. 3. Clé utilisée en cryptographie à clé publique qui appartient à une entité individuelle et est distribuée publiquement. Les autres entités utilisent cette clé pour chiffrer les données à envoyer au propriétaire de la clé.	X.509 X.810 J.170
Certificat de clé publique (*public key certificate*)	1. Clé publique d'un utilisateur, associée à certaines autres informations qui sont rendues non falsifiables par chiffrement en utilisant la clé privée de l'autorité de certification émettrice. 2. Valeurs représentant une clé publique de détenteur (et d'autres informations facultatives), ces valeurs ayant été vérifiées et signées par une autorité de confiance sous une forme infalsifiable. 3. Relation entre la clé publique d'une entité et un ou plusieurs attributs relatifs à son identité, également appelé certificat numérique.	X.509 H.235 J.170
Cryptographie à clé publique (*public key cryptography*)	Technique cryptographique fondée sur un algorithme à deux clés (publique et privée), dans laquelle un message est chiffré avec la clé publique mais ne peut être déchiffré qu'au moyen de la clé privée. Egalement appelé système PPK (clé privée-publique). Note – Le fait de connaître la clé publique ne permet pas d'en déduire la clé privée. Par exemple, le correspondant A construit une clé publique et une clé privée de ce type. Il envoie la clé publique sans restriction à tous ceux qui souhaitent communiquer avec lui, mais il garde la clé privée secrète. Tous ceux qui possèdent la clé publique peuvent alors crypter un message pour le correspondant A, mais seul celui-ci peut décrypter ces messages, à l'aide de sa clé privée.	J.93
Infrastructure de clé publique (PKI, *public key infrastructure*)	Infrastructure pouvant prendre en charge la gestion de clés publiques afin de fournir des services d'authentification, de chiffrement, d'intégrité et de non-répudiation.	X.509

Terme	Définition	Référence
Autorité d'enregistrement (RA, *registration authority*)	1. Entité responsable de l'identification et de l'authentification des sujets de certificats, qui n'est néanmoins ni une autorité de certification ni une autorité en charge des attributs, et par conséquent ne signe ni ne délivre de certificats. Note – Une autorité d'enregistrement peut apporter son aide au cours des processus de demande de certificat ou de révocation ou des deux. 2. Autorité habilitée et chargée en toute confiance d'exécuter un service d'enregistrement.	X.842 X.843
Attaque par relais (*relay attack*)	Attaque visant l'authentification caractérisée par le fait que des informations AI pour échange sont interceptées puis immédiatement réexécutées.	X.811
Participant faisant confiance (*relying party*)	Utilisateur ou agent qui fait confiance aux données contenues dans un certificat pour prendre des décisions.	X.509
Répétition (*replay*)	Un message ou une partie d'un message est répété pour produire un effet non autorisé. Par exemple, un message valide contenant des informations d'authentification peut être répété par une autre entité pour s'authentifier elle-même (comme quelque chose qu'elle n'est pas).	X.800
Répudiation (*repudiation*)	1. Le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie. 2. Une entité nie son implication dans un échange de communication antérieur. 3. (Dans un système MHS, c'est) quand un utilisateur du système MTS ou le système MTS ont ultérieurement la possibilité de refuser le dépôt, la réception ou l'expédition d'un message. Les risques de répudiation sont les suivants: refus d'origine, refus de dépôt, refus de remise.	X.800 M.3016.0 X.402
Révélation (*reveal*)	Opération qui supprime une partie ou la totalité de la protection par confidentialité appliquée précédemment.	X.814
Certificat de révocation (*revocation certificate*)	Certificat de sécurité émis par une autorité de sécurité pour indiquer qu'un certificat de sécurité particulier a été révoqué.	X.810
Certificat de révocation de liste (*revocation list certificate*)	Certificat de sécurité qui identifie une liste de certificats de sécurité qui ont été révoqués.	X.810
Contrôle de routage (*routing control*)	Application de règles, au cours du processus de routage, afin de choisir ou d'éviter, des réseaux, liaisons ou relais spécifiques.	X.800
Politique de sécurité fondée sur des règles (*rule-based security policy*)	Politique de sécurité fondée sur des règles globales imposées à tous les utilisateurs. Ces règles s'appuient généralement sur une comparaison de la sensibilité des ressources auxquelles on doit accéder avec les attributs correspondants d'utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs.	X.800
Scellé (*seal*)	Valeur de contrôle cryptographique qui met en œuvre l'intégrité mais qui ne protège pas d'une falsification du récepteur (c'est-à-dire qu'il n'offre pas la non-répudiation). Lorsqu'un scellé est associé à un élément de données, cet élément de données est dit *scellé*. *Note* –Bien qu'un scellé n'offre pas lui-même la non-répudiation, certains mécanismes de non-répudiation font usage du service d'intégrité offert par les scellés, par exemple, pour protéger les communications avec des tierces parties de confiance.	X.810
Clé secrète (*secret key*)	Clé qui est utilisée avec un algorithme symétrique de cryptographie. La possession de cette clé est limitée (habituellement à deux entités).	X.810
Sécurité (*security*)	Le terme "*sécurité*" est utilisé dans le sens d'une minimisation des vulnérabilités d'actifs et de ressources. Un actif est tout élément de valeur. Une *vulnérabilité* est toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient. Une *menace* est une violation potentielle de la sécurité.	X.800
Administrateur de sécurité (*security administrator*)	Personne qui est responsable de la définition ou de l'application d'une ou de plusieurs parties de la politique de sécurité.	X.810
Alarme de sécurité (*security alarm*)	Message généré lorsqu'un événement lié à la sécurité, défini par la politique de sécurité comme étant une condition d'alarme, a été détecté. Une alarme de sécurité est destinée à être portée à temps à l'attention d'entités appropriées.	X.816

Terme	Définition	Référence
Association de sécurité (*security association*)	Relation entre deux ou plus de deux entités pour lesquelles il existe des attributs (règles et informations d'état) régissant la fourniture des services de sécurité qui intéressent les entités en question. Relation établie entre des entités communicantes de couches inférieures pour laquelle sont définis les attributs d'association de sécurité correspondants.	X.803 X.802
Audit de sécurité (*security audit*)	Revue indépendante et examen des enregistrements et des activités du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures.	X.800
Journal d'audit de sécurité (*security audit trail*)	Données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité.	X.800
Agent d'audit de sécurité (*security auditor*)	Individu ou processus autorisé à avoir accès au journal de sécurité et à bâtir des rapports d'audit.	X.816
Autorité de sécurité, autorité chargée de la sécurité (*security authority*)	1. Entité qui est responsable de la définition, de l'implémentation ou de l'application de la politique de sécurité. 2. Entité responsable auprès de l'administration de la politique de sécurité dans un domaine de sécurité. 3. Administrateur responsable de l'implémentation d'une politique de sécurité.	X.810 X.841 X.903
Certificat de sécurité (*security certificate*)	Ensemble de données relatives à la sécurité émis par une autorité de sécurité ou une tierce partie de confiance ainsi que les informations de sécurité qui sont utilisées pour fournir des services d'intégrité et d'authentification de l'origine des données. *Note* – Tous les certificats sont réputés être des certificats de sécurité. Le terme *certificat de sécurité* est adopté dans la série X.800 afin d'éviter des conflits de terminologie avec la Rec. UIT-T X.509.	X.810
Domaine de sécurité (*security domain*)	1. Ensemble d'utilisateurs et de systèmes faisant l'objet de l'application d'une politique de sécurité commune. 2. Ensemble de ressources associé à une politique de sécurité unique.	X.841 X.411
Echange pour la sécurité (*security exchange*)	Transfert ou séquence de transferts d'informations de contrôle de protocole d'application entre systèmes ouverts, faisant partie intégrante d'un ou de plusieurs mécanismes de sécurité.	X.803
Information de sécurité (SI, *security information*)	Information nécessaire pour implémenter des services de sécurité.	X.810
Etiquette de sécurité (*security label*)	Marque liée à une ressource dénommant ou désignant les attributs de sécurité de cette ressource (cette ressource peut être une unité de données).	X.800
Gestion de la sécurité (*security management*)	La gestion de la sécurité englobe toutes les activités d'établissement, de maintien et de terminaison de caractéristiques de sécurité d'un système. Les sujets suivants sont traités: gestion de services de sécurité; installation de mécanismes de sécurité; gestion des clés (partie de gestion); établissement d'informations d'identité, de clés, de contrôle d'accès, etc.; gestion de la trace de l'audit de sécurité et des alarmes de sécurité.	M.3016.0
Modèle de sécurité (*security model*)	Cadre pour décrire les services de sécurité destinés à faire face aux éventuelles menaces visant le système MTS et les éléments de sécurité qui sont à la base de ces services.	X.402

Terme	Définition	Référence
Politique de sécurité (*security policy*)	1. Ensemble de règles fixées par l'autorité de sécurité qui régit l'utilisation et la fourniture de services et de fonctionnalités de sécurité. 2. Ensemble des critères permettant de fournir des services de sécurité. *Note* – Voir aussi politique de sécurité fondée sur l'identité (*identity-based security policy*) et politique de sécurité fondée sur des règles (*rule-based security policy*). Une politique de sécurité complète traite nécessairement de sujets qui ne relèvent pas du champ d'application de l'OSI.	X.509 X.800
Règles de sécurité (*security rules*)	Information locale qui, pour les services de sécurité choisis, spécifie les mécanismes de sécurité sous-jacents à utiliser, y compris l'ensemble des paramètres nécessaires au fonctionnement de ces mécanismes. *Note* – Les règles de sécurité sont une forme de règles d'interaction sûres telles que celles-ci sont définies dans le Modèle de sécurité pour les couches supérieures.	X.802
Service de sécurité (*security service*)	Service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données.	X.800
Etat de sécurité (*security state*)	Informations d'état conservées dans un système ouvert et nécessaires à la fourniture des services de sécurité.	X.803
Jeton de sécurité (*security token*)	Ensemble de données protégé par un ou plusieurs services de sécurité, ainsi que les informations de sécurité utilisées pour la fourniture de ces services de sécurité, qui est transféré entre les entités communicantes.	X.810
Transformation pour la sécurité (*security transformation*)	Ensemble de fonctions (fonctions de sécurité de système et fonctions de communication de sécurité) qui agissent en combinaison sur les éléments de données d'usager pour en assurer la protection dans des conditions spécifiques pendant la communication ou le stockage.	X.803
Protection sélective des champs (*selective field protection*)	Protection de certains champs spécifiques dans un message à transmettre.	X.800
Sensibilité (*sensitivity*)	Caractéristique d'une ressource liée à sa valeur ou à son importance.	X.509
Secret partagé (*shared secret*)	Clé de sécurité pour les algorithmes cryptographiques; le secret partagé peut être déduit d'un mot de passe.	H.530
Protection (*shield*)	Conversion de données en données protégées par l'intégrité.	X.815
Signature	Voir signature numérique (*digital signature*).	X.800
Authentification simple (*simple authentication*)	Authentification utilisant de simples accords de mot de passe.	X.509
Source d'autorité (SOA, *source of authority*)	Autorité d'attribut auquel peut faire confiance un vérificateur de privilège pour une ressource donnée, en tant qu'autorité ultime pour l'attribution d'un ensemble de privilèges.	X.509
Spamming, submersion (*spamming*)	Agression visant à amener un système à une situation de refus de service par l'envoi, à celui-ci, d'un grand nombre de données non autorisées. Un cas particulier est la submersion d'un média par l'envoi de paquets RTP à des ports UDP. Généralement, le système est submergé de paquets et le traitement correspondant nécessite de précieuses ressources.	H.235
Authentification forte (*strong authentication*)	Authentification utilisant des justificatifs obtenus par des moyens de chiffrement.	X.509
Méthode d'authentification symétrique (*symmetric authentication method*)	Méthode dans laquelle les deux entités partagent des informations d'authentification communes.	X.811

Terme	Définition	Référence
Algorithme symétrique de cryptographie (*symmetric cryptographic algorithm*)	Algorithme pour réaliser le chiffrement ou algorithme pour réaliser le déchiffrement correspondant dans lequel la même clé est requise à la fois pour le chiffrement et le déchiffrement.	X.810
Menace (*threat*)	Violation potentielle de la sécurité.	X.800
Service d'horodatage (*time stamping service*)	Service attestant de l'existence d'une donnée électronique à un moment précis dans le temps. *Note* – Les services d'horodatage sont utiles et probablement indispensables pour prendre à charge la validation à long terme de signatures.	X.842
Analyse du trafic (*traffic analysis*)	Déduction d'informations à partir de l'observation des flux de données (présence, absence, quantité, direction, fréquence).	X.800
Confidentialité du flux de données (*traffic flow confidentiality*)	Service de confidentialité fournissant une protection contre l'analyse du trafic, autrement dit un service de sécurité assurant la protection des informations qui pourraient être dérivées de l'observation des flux de données.	X.800
Bourrage (*traffic padding*)	Production d'instances de communication parasites, d'unités de données parasites et/ou de données parasites dans des unités de données.	X.800
Trappes (*trapdoor*)	Résultat d'une action dans laquelle une entité d'un système est modifiée pour permettre à un attaquant de produire un effet non autorisé sur demande ou lors d'un événement ou d'une séquence d'événements prédéterminés. Par exemple, une validation de mot de passe pourrait être modifiée de façon à valider également le mot de passe d'un attaquant, en plus de son effet normal.	X.800
Cheval de Troie (*Trojan horse*)	Un "cheval de Troie" est un programme introduit dans le système avec une fonction non autorisée, en plus de sa fonction autorisée. Un relais qui copie également des messages à destination d'une voie non autorisée est un "cheval de Troie".	X.800
Confiance (*trust*)	On dit que l'entité X *fait confiance* à l'entité Y pour un ensemble d'activités si et seulement si l'entité X suppose que l'entité Y se comportera d'une certaine façon par rapport aux activités.	X.810
Entité de confiance (*trusted entity*)	Entité qui peut violer une politique de sécurité, soit en réalisant des actions qu'elle n'est pas censée accomplir, soit en ne réussissant pas à réaliser des actions qu'elle est censée accomplir.	X.810
Fonctionnalité de confiance (*trusted functionality*)	Fonctionnalité perçue comme correcte en ce qui concerne certains critères, tels que ceux qui sont définis par une politique de sécurité, par exemple.	X.800
Tierce partie de confiance (TTP, *trusted third party*)	Autorité de sécurité ou son agent auquel [d'autres entités font] confiance au regard de certaines activités liées à la sécurité (dans le contexte d'une politique de sécurité).	X.810
Accès non autorisé (*unauthorized access*)	Une entité tente d'accéder à des données en violation de la politique de sécurité en vigueur.	M.3016.0
Retrait de l'intégrité (*unshield*)	Conversion de données protégées par l'intégrité en données initialement protégées.	X.815
Authentification de l'utilisateur (*user authentication*)	Fourniture de la preuve de l'identité d'un utilisateur humain ou d'un processus d'application.	M.3016.0
Validation (*validate*)	Vérification de données protégées par l'intégrité pour détecter une perte d'intégrité.	X.815
Vérificateur (*verifier*)	Entité qui est ou qui représente l'entité revendiquant une identité authentifiée. Un vérificateur comporte les fonctions nécessaires pour engager des échanges pour authentification.	X.811
Vulnérabilité (*vulnerability*)	Toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient.	X.800
Certificat X.509 (*X.509 certificate*)	Spécification de certificat de clé publique élaborée dans le cadre de la norme d'annuaire X.500 de l'UIT-T.	J.170

B.2 Acronymes relatifs à la sécurité

Acronyme	Définition
AA	[X.509] Autorité d'attribut (*attribute authority*)
ACI	[SANCHO] Information de contrôle d'accès (*access control information*)
AE	[M.3010] Entité d'application (*application entity*)
AES	[H.235] [J.170] Norme de chiffrement perfectionné (*advanced encryption standard algorithm*)
APS	[SANCHO] Commutation de protection automatique (*automatic protection switching*)
ASN.1	[X.680] Notation de syntaxe abstraite numéro un (*abstract syntax notation one*)
ASON	[SANCHO] Réseau optique à commutation automatique (*automatically switched optical network*)
ASP	[X.805] [X.1121] Fournisseur de services d'application (*application service provider*)
CA	[H.234] [H.235] [J.170] [X.509] Autorité de certification (*certification authority*). Il s'agit d'une organisation de confiance qui accepte les demandes de certificat provenant des entités, authentifie les demandes, émet les certificats et tient à jour les informations d'état concernant les certificats. [J.170] agent d'appel (call agent). Il s'agit de la partie du serveur CMS qui maintient l'état de communication et contrôle le côté ligne de la communication.
CME	[X.790] Entité de gestion conforme (*conformant management entity*)
CMIP	[M.3010] Protocole commun d'informations de gestion (*common management information protocol*)
CMS	[J.170] Syntaxe des messages cryptographiques (*cryptographic message syntax*). [J.170] Serveur de gestion d'appels (*call management server*), qui contrôle les connexions audio. Egalement appelé agent d'appel dans la terminologie MGCP/SGCP (c'est un exemple de serveur d'application).
CORBA	[SANCHO] Architecture de courtier de requêtes pour objets commun (*common object request broker architecture*)
COS	[SANCHO] Classe de service (*class of service*)
CP	Politique de certificat (*certificate policy*)
CPS	[SANCHO: X.842] Déclaration de méthode de certification (*certification practice statement*) [SANCHO: Q.817] Déclaration de politique de certification (*certification policy statement*)
CRL	[H.235] [X.509] Liste de révocation de certificats (*certificate revocation list*)
DES	[SANCHO] Norme de chiffrement des données, norme de chiffrement numérique (*data encryption standard, digital encryption standard*)
DHCP	[SANCHO] Protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DOCSIS	[SANCHO] Spécification d'interface du service de transmission de données par câble (*data-over-cable service interface specification*)
DSA	[X.509] Agent de système d'annuaire (*directory system agent*) [SANCHO] Algorithme de signature numérique (*digital signature algorithm*)
DSL	[SANCHO] Boucle d'abonné numérique (*digital subscriber loop*)
DSP	[SANCHO] Processeur de signaux numériques (*digital signal processor*) [SANCHO] Protocole du système d'annuaire (*directory system protocol*)
FDS	[SANCHO] Système de détection des fraudes (*fraud detection system*)
FEAL	[T.36] L'algorithme de chiffrement de données rapide (*fast data encipherment algorithm*) est une famille d'algorithmes qui convertit chaque bloc de texte en clair de 64 bits en un bloc de texte chiffré de 64 bits à l'aide d'une clé secrète de 64 bits. Il est analogue à l'algorithme DES mais comporte une fonction f beaucoup plus simple. Il a été conçu pour être rapide et simple, afin d'être adapté aux microprocesseurs peu complexes (par exemple les cartes à puce). (Voir A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997.)
FIGS	[M.3210.1] Système de collecte des informations de fraude (*fraud information gathering system*)
GK	[H.235] [H.510] [H.530] Portier (*gatekeeper*)
GW	[H.235] Passerelle (*gateway*)

Acronyme	Définition
HFC	[SANCHO] Système hybride fibre optique/câble coaxial (*hybrid fibre-coaxial cable*)
HFX	[T.30] [T.36] Chiffrement de télécopie de Hawthorne (*hawthorne facsimile cipher*)
HKM	[T.30] [T.36] Algorithme de gestion de clés de Hawthorne (*hawthorne key management algorithm*)
ICN	Réseau d'information et de communication (*information and communication network*)
ID	[H.235] Identificateur (*identifier*)
IDEA	[T.36] L'algorithme international de chiffrement de données (*international data encryption algorithm*) est un algorithme de chiffrement créé par Xuejia Lai et James Massey en 1992 qui utilise un chiffrement par blocs avec une clé de 128 bits (blocs de 64 bits avec une clé de 128 bits) et qui est généralement considéré comme étant très sûr. Il est considéré comme faisant partie des meilleurs algorithmes publics. Pendant les quelques années au cours desquelles il a été utilisé, aucune attaque véritable n'a été signalée malgré un grand nombre de tentatives (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html).
IKE	[J.170] L'échange de clés Internet (*Internet key exchange*) est un mécanisme de gestion de clés utilisé pour négocier et obtenir des clés pour des associations de sécurité (SA) dans le protocole IPSec.
IKE–	[J.170] Notation désignant l'utilisation du mécanisme IKE avec des clés préalablement partagées pour l'authentification.
IKE+	[J.170] Notation désignant le mécanisme IKE nécessitant des certificats de clé publique.
IMT-2000	[M.3210.1] Télécommunications mobiles internationales 2000 (*international mobile telecommunications 2000*)
IP	[X.805] Protocole Internet (*Internet protocol*)
IPSec	[H.235] [H.530] [J.170] [X.805] Sécurité du protocole Internet (*Internet protocol security*).
IVR	[J.170] Système à réponse vocale interactive (*interactive voice response system*)
LAN	[M.3010] Réseau local (*local area network*)
LDAP	[H.235] Protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)
LLA	[M.3010] Architecture logique répartie en couches (*logical layered architecture*)
MAC	[H.235] [J.170] Code d'authentification de message (*message authentication code*). Il s'agit d'un élément de données de longueur fixe qui est envoyé conjointement avec un message pour en garantir l'intégrité, également appelé MIC. [J.170] Commande d'accès au support (*media access control*). C'est une sous-couche de la couche liaison de données. Elle se trouve normalement directement au-dessus de la couche physique.
MCU	[H.235] Unité de multidiffusion (*multicast unit*) [H.323] Pont de conférence/unité de commande multipoint (*multipoint control unit*)
MD-5	[H.235] [J.170] Condensé de message N° 5 (*message digest No. 5*)
MG	[J.170] Passerelle média (*media gateway*)
MGC	[J.170] Contrôleur de passerelle média (*media gateway controller*)
MGCP	[J.170] Protocole de commande de passerelle média (*media gateway control protocol*)
MIB	[J.170] [M.3010] Base d'informations de gestion (*management information base*)
MIS	[M.3010] Système d'informations de gestion (*management information system*)
MS	[M.3210.1] Système de gestion (*management system*) Mémoire de messages (*message store*) Section de multiplexage (*multiplex section*)
MSP	[SANCHO] Protection de section de multiplexage (*multiplex section protection*)
MS-SPRing	Anneau à protection partagée de section de multiplexage (*multiplex section shared protection ring*)
MTA	[J.170] Adaptateur de terminal média (*media terminal adapter*) Adaptateur de terminal multimédia (*multimedia terminal adapter*) Agent de transfert de messages (*message transfer agent*)
NAT	[H.235] Traduction d'adresse de réseau (*network address translation*)
OAM&P	[SANCHO] Exploitation, administration, maintenance et fourniture (*operations, administration, maintenance & provisioning*)

Acronyme	Définition
OS	[M.3010] [X.790] Système d'exploitation (*operations system*)
OSF	[M.3010] Fonction de système d'exploitation (*operations systems function*)
OSI	[SANCHO] Interconnexion des systèmes ouverts (*open systems interconnection*)
OSS	[J.170] Système d'assistance à l'exploitation (*operation system support*). Il s'agit des logiciels d'arrière utilisés pour la gestion de la configuration, de la qualité de fonctionnement, des défauts, de la comptabilité et de la sécurité.
PDA	Assistant personnel électronique (*personal data assistant*)
PKI	[H.235] [H.530] [X.509] [J.170] Infrastructure de clé publique (*public key infrastructure*). Processus permettant d'émettre des certificats de clé publique, incluant des normes, des autorités de certification, une communication entre autorités et des protocoles de gestion des processus de certification.
PKINIT	[J.160] [J.191] Authentification initiale par cryptographie à clé publique (*public key cryptography initial authentication, public-key cryptography for initial authentication*)
PMI	[X.509] Infrastructure de gestion de privilège (*privilege management infrastructure*)
QS	[SANCHO] Qualité de service
RA	Autorité d'enregistrement (*registration authority*)
RADIUS	[J.170] Service utilisateur d'authentification par téléphone (*remote authentication dial-in user service*)
RAS	[SANCHO] Enregistrement, admission et statut (*registration, admission and status*) [SANCHO] Protocole d'enregistrement, admission et statut (*registration, admission and status protocol*)
RBAC	[X.509] Contrôle d'accès basé sur des règles (*rule-based access control*)
RCD	[SANCHO] Réseau de communication de données
RGT	[M.3010] [M.3210.1] [X.790] Réseau de gestion des télécommunications
RKS	[J.170] Serveur d'archivage (*record keeping server*). Dispositif qui collecte et corrèle les divers messages d'événement.
RSA	[H.235] [T.30] [T.36] Rivest, Shamir et Adleman (algorithme à clé publique)
RTP	[H.225.0] [H.235] [J.170] Protocole de transport en temps réel (*real time protocol*)
SHA-1	[H.235] Algorithme de hachage sécurisé N° 1 (*secure hash algorithm No.1*)
SG	Passerelle de signalisation (*signalling gateway*)
SIP	[J.170] [X.805] Protocole d'ouverture de session (*session initiation protocol*). Protocole (de signalisation) de commande de la couche application permettant de créer, de modifier et de terminer des sessions avec un ou plusieurs participants.
SNC	[SANCHO] Connexion de sous-réseau (*sub-network connection*)
SNMP	[J.170] [X.805] Protocole simple de gestion de réseau (*simple network management protocol*)
SoA	[X.509] Source d'autorité (*source of authority*)
SRTP	[H.235] Protocole de transport en temps réel sécurisé (*secure real time protocol*)
SS7	[J.170] [X.805] Le Système de signalisation N° 7 (*signalling system number 7*) est une architecture et un ensemble de protocoles assurant la signalisation d'appel hors bande dans un réseau téléphonique.
SSL	[H.235] [X.805] Couche de connexion sécurisée (*secure socket layer*)
TFTP	[SANCHO] Protocole trivial de transfert de fichiers (*trivial file transfer protocol*)
TGS	[J.160] Serveur-distributeur de tickets (*ticket granting server*)
TIC	Technologies de l'information et de la communication
TLS	[H.235] Sécurité de la couche transport (*transport level security*)
TTP	[X.810] Tiers de confiance (*trusted third party*)
UDP	[J.170] Protocole datagramme d'utilisateur (*user datagram protocol*)
VA	Autorité de validation (*validation authority*)
VoIP	[X.805] Téléphonie IP, voix sur IP (*voice over IP*)
VPN	[X.805] Réseau privé virtuel (*virtual private network*)

Annexe C

Liste des commissions d'études et des Questions liées à la sécurité

Le travail de normalisation de l'UIT-T est effectué par les commissions d'études (CE), au sein desquelles des représentants des membres de l'UIT-T élaborent des Recommandations (normes) dans les divers domaines des télécommunications internationales. Ce travail s'articule autour de Questions mises à l'étude. Chacune de ces Questions porte sur des études techniques à réaliser dans un domaine particulier de la normalisation des télécommunications. Ci-après sont énumérées les commissions d'études de l'UIT-T pour la période d'études 2005-2008 avec leur titre, leur mandat et les Questions à l'étude dans le domaine de la sécurité.

CE 2	Aspects opérationnels de la fourniture du service, réseaux et qualité de fonctionnement *Commission d'études directrice pour la définition des services, le numérotage et l'acheminement*
Etudes se rapportant aux principes de fourniture du service, à la définition et aux critères opérationnels de l'émulation de service; aux prescriptions de numérotage, de nommage et d'adressage et à l'assignation des ressources, en particulier aux critères et procédures à suivre pour la réservation et l'assignation; aux prescriptions de routage et d'interfonctionnement; aux facteurs humains; aux aspects opérationnels des réseaux et aux critères de qualité de fonctionnement associés, en particulier la gestion du trafic du réseau, la qualité de service (ingénierie du trafic, qualité de fonctionnement opérationnelle et mesures en service); aux aspects opérationnels de l'interfonctionnement entre réseaux de télécommunication classiques et nouveaux réseaux; à l'évaluation des informations en retour des opérateurs, des équipementiers et des utilisateurs sur différents aspects de l'exploitation du réseau.	
Questions liées à la sécurité:	
– **Q.1/2** – Application des plans de numérotage, de nommage et d'adressage aux télécommunications, et aspects de service et d'exploitation du numérotage, y compris la définition des services (F.851)	
– **Q.4/2** – Aspects opérationnels de la qualité de service des réseaux de télécommunication (E.408, E.409 (conjointement avec la CE 17))	

CE 3	Principes de tarification et de comptabilité et questions connexes de politique générale et d'économie des télécommunications
Etudes se rapportant aux principes de tarification et de comptabilité pour les services internationaux de télécommunication et étude des questions connexes d'économie et de politique générale des télécommunications. A cette fin, la Commission d'études 3 encouragera en particulier la collaboration entre ses membres en vue de fixer des taux à des niveaux aussi bas que possible dans un souci d'efficacité du service et en tenant compte de la nécessité de conserver une gestion financière indépendante des télécommunications sur une base saine.	
Questions liées à la sécurité: Aucune	

CE 4	Gestion des télécommunications *Commission d'études directrice pour la gestion des télécommunications*

Etudes se rapportant à la gestion des services, réseaux et équipements de télécommunication, y compris la prise en charge des réseaux de prochaine génération (NGN), ainsi qu'à l'application et à l'évolution du cadre général du réseau de gestion des télécommunications (RGT). Cette commission est également responsable d'autres études de gestion des télécommunications se rapportant aux désignations, aux procédures d'exploitation propres au transport et aux techniques et instruments de test et de mesure.

Les études sur la sécurité menées par la CE 4 en tant que Commission d'études directrice pour les activités de gestion concernent les domaines suivants:

a) considérations et spécifications relatives à l'architecture des interfaces de gestion;

b) spécifications détaillées visant à sécuriser le réseau de gestion (également appelé plan de gestion), compte tenu notamment de la convergence actuelle des réseaux;

c) protocole et modèles relatifs à la sécurisation des informations de gestion et à la gestion des paramètres de sécurité.

La gestion du réseau de télécommunications est définie à différents niveaux d'abstraction, depuis la gestion des informations au niveau des éléments de réseau jusqu'aux services de gestion offerts au client. Les spécifications de sécurité pour les informations échangées entre systèmes de gestion ainsi qu'entre systèmes de gestion et éléments de réseau dépendent de la question de savoir si les réseaux de gestion relèvent d'une seule administration ou de plusieurs. Sur la base des principes architecturaux, des spécifications, mécanismes et protocoles explicites ont été définis dans des Recommandations existantes et d'autres sont en cours d'élaboration.

La série M.3016 approuvée récemment remplace la Rec. UIT-T M.3016 initiale (1998). Elle décrit l'importance et l'applicabilité de la sécurité dans le contexte du RGT. Plutôt que de spécifier un ensemble de services pour la protection contre les menaces, elle définit un cadre que les différents organismes peuvent utiliser pour spécifier correctement l'utilisation des mécanismes disponibles.

La série M.3016 porte sur les menaces suivantes dans le RGT: usurpation d'identité, écoute clandestine, accès non autorisé, perte ou altération d'informations, répudiation, falsification et déni de service. Elle porte aussi sur les fonctionnalités de sécurité suivantes: confidentialité, intégrité des données, responsabilité et disponibilité.

Questions liées à la sécurité:

– **Q.6/4** – Principes et architecture de gestion (M.3010, série M.3016, M.3400)

– **Q.7/4** – Prescriptions relatives aux interfaces de gestion entreprise-entreprise et particulier-entreprise (M.3320)

– **Q.10/4** – Modèles informationnels propres aux applications (M.3210.1)

– **Q.11/4** – Protocoles pour les interfaces de gestion (Q.813, Q.815, Q.817)

CE 5	Protection contre les effets dus à l'environnement électromagnétique
Etudes se rapportant à la protection des réseaux et équipements de télécommunication contre les brouillages et la foudre. La commission est également chargée des études relatives à la compatibilité électromagnétique (CEM) et aux conséquences, sur la sécurité et la santé, des champs électromagnétiques produits par les installations et dispositifs de télécommunication, y compris les téléphones cellulaires.	
Pour remplir sa mission, la CE 5 étudie plusieurs Questions et élabore des Recommandations et Manuels permettant de contribuer à la sécurité du réseau contre les menaces électromagnétiques (par exemple les phénomènes malveillants d'origine humaine de transitoires à puissance élevée tels que les impulsions électromagnétiques à haute altitude (HEMP, *high-altitude electromagnetic pulse*)) et les hyperfréquences à puissance élevée (HPM, *high-power microwave*). Dans le cadre de la sécurité électromagnétique, on s'intéresse également aux fuites d'informations des réseaux de télécommunication dues aux rayonnements imprévus des équipements.	
La nature des menaces malveillantes et les techniques d'atténuation correspondantes sont analogues à celles qui s'appliquent aux perturbations électromagnétiques naturelles ou non intentionnelles. Il existe des analogies entre les impulsions HEMP et les impulsions électromagnétiques créées par la foudre. Les techniques d'occultation et de filtrage qui permettent aux équipements de réduire leurs rayonnements non désirés permettent aussi de réduire le risque de fuite d'énergie non intentionnelle. Les activités traditionnelles de la Commission d'études 5 relatives à la protection contre la foudre et au contrôle des brouillages électromagnétiques contribuent donc à la sécurité du réseau contre les menaces malveillantes d'origine humaine. Au cours de la période d'études actuelle, les aspects des travaux de la Commission d'études relatifs à la sécurité sont abordés dans le cadre de la nouvelle Question 15/5 (*Sécurité des systèmes de télécommunication et d'information en ce qui concerne l'environnement électromagnétique*).	
Les menaces électromagnétiques comprennent les phénomènes malveillants d'origine humaine de transitoires à puissance élevée tels que les impulsions électromagnétiques à haute altitude (HEMP, *high-altitude electromagnetic pulse*) et les émissions provenant de générateurs électromagnétiques à puissance élevée (HPEM, *high-power electromagnetic*), y compris les sources d'hyperfréquences à puissance élevée (HPM, *high-power microwave*) et les sources à ultra large bande (UWB, ultra-wideband). Par ailleurs, dans le cadre de la sécurité électromagnétique, il faut s'intéresser aux fuites d'informations des réseaux de télécommunication dues aux rayonnements imprévus des équipements.	
Questions liées à la sécurité:	
– **Q.2/5** – Compatibilité CEM liée aux réseaux d'accès large bande (*Le contrôle des rayonnements non désirés des systèmes d'accès à large bande contribue à réduire le risque de fuites d'informations*).	
– **Q.4/5** – Résistance des équipements de communication (*La résistance des équipements à la foudre permet d'améliorer la résistance des équipements aux surtensions induites par les impulsions HEMP*).	
– **Q.5/5** – Protection contre la foudre des systèmes de télécommunication (*Les techniques utilisées pour la protection contre la foudre permettent également de renforcer la protection des équipements contre les impulsions HEMP et les rayonnements HPE*).	
– **Q.6/5** – Configurations d'équipotentialité et mise à la terre des systèmes de télécommunication dans l'environnement mondial (*Des mesures appropriées relatives à l'équipotentialité et à la mise à la Terre permettent également de renforcer la protection des équipements contre les impulsions HEMP et les rayonnements HPE*).	
– **Q.12/5** – Mise à jour et amélioration des Recommandations existantes relatives à la compatibilité CEM (*La compatibilité électromagnétique des équipements de télécommunication améliore leur immunité aux impulsions HEMP conduites et rayonnées ainsi qu'aux rayonnements HPE. Elle réduit par ailleurs le risque de fuites d'informations*).	
– **Q.15/5** – Sécurité des systèmes de télécommunication et d'information en ce qui concerne l'environnement électromagnétique (*La résistance des équipements à la foudre améliore leur résistance aux surtensions induites par les impulsions HEMP*).	

CE 6	Installations extérieures et installations intérieures connexes
Etudes se rapportant aux installations extérieures et aux installations intérieures connexes telles que: construction, installation, raccordement, terminaison et protection contre la corrosion et les autres formes de dommages causés par l'environnement, à l'exception des phénomènes électromagnétiques, de tous les types de câble terrestres pour les télécommunications publiques et des structures associées.	
Questions liées à la sécurité:	
– **Q.1/6** – Procédures relatives à l'environnement et à la sécurité des installations extérieures	
– **Q.6/6** – Maintenance des réseaux de câbles à fibres optiques	

CE 9	Réseaux en câble intégrés à large bande et transmission télévisuelle et sonore *Commission d'études directrice pour les réseaux de télévision et câblés intégrés large bande.*
Etudes se rapportant: a) à l'utilisation des réseaux en câble et des réseaux hybrides conçus avant tout pour la distribution chez le particulier de programmes de télévision et de programmes radiophoniques, par exemple réseaux intégrés à large bande pour acheminer les services vocaux et d'autres services à paramètre temps critique, la vidéo à la demande et les services interactifs, etc.; b) à l'utilisation des systèmes de télécommunication pour la contribution, la distribution primaire et la distribution secondaire de programmes de télévision, de programmes radiophoniques et de services de données similaires.	
En tant que Commission d'études directrice pour les réseaux de télévision et câblés intégrés large bande, la CE 9 évalue les menaces et les vulnérabilités relatives aux réseaux et services à large bande, définit des objectifs de sécurité, évalue les contre-mesures et définit des architectures de sécurité.	
Les activités relatives à la sécurité portent essentiellement sur:	
a) *Les services de sécurisation de l'accès large bande:* services de sécurité pour les réseaux d'accès à large bande, à savoir authentification du câblo-modem, gestion des clés de chiffrement, confidentialité et intégrité des données transmises et téléchargement sécurisé de logiciels de câblo-modem.	
b) *Les services de sécurisation de la téléphonie IP:* IPCablecom est un projet spécial sur la fourniture de services interactifs à temps critique sur le réseau de transmission de télévision par câble au moyen du protocole IP, en particulier la voix et la vidéo sur IP. Les services de sécurité offerts dans le réseau IPCablecom comprennent l'authentification de l'adaptateur de terminal multimédia (MTA, *multimedia terminal adapter*) auprès du fournisseur de services, l'authentification du fournisseur de services auprès de l'adaptateur MTA, la fourniture et la configuration sécurisées des dispositifs, la gestion sécurisée des dispositifs, la transmission sécurisée de la signalisation et la transmission sécurisée des médias.	
c) *Les services de sécurisation des connexions de réseau domestiques:* des câblo-modems améliorés peuvent offrir des services de réseau domestique tels que des pare-feu ou la traduction d'adresse de réseau. Les services de sécurité prévus pour les câblo-modems améliorés comprennent l'authentification de l'adaptateur de terminal multimédia (MTA, *multimedia terminal adapter*) auprès du fournisseur de services, l'authentification du fournisseur de services auprès de l'adaptateur MTA, la fourniture et la configuration sécurisée des dispositifs, la gestion sécurisée des dispositifs, la fonctionnalité de pare-feu/filtrage de paquets, la gestion sécurisée des pare-feu et le téléchargement sécurisé de logiciels de câblo-modems améliorés.	
d) Les environnements applicatifs sécurisés pour les services de télévision interactive: les services de télévision interactive s'appuient sur les services de sécurité définis en Java et sur la spécification de la plate-forme domestique multimédia (MHP, multimedia home platform).	

Questions liées à la sécurité:
– **Q.3/9** – Méthodes et pratiques applicables à l'accès conditionnel et à la protection contre les copies illicites et contre la redistribution illicite ("contrôle de redistribution" pour la télévision numérique par câble à domicile) (J.93, J.96)
– **Q.8/9** – Acheminement sur le réseau de télévision par câble de services et applications numériques utilisant des protocoles Internet (IP) et/ou de données en mode paquet (J.112)
– **Q.9/9** – Applications vocales et vidéo de type IP sur des réseaux de télévision par câble (J.160, J.170, J.191)
– **Q.10/9** – Extension des services par câble à large bande sur les réseaux domestiques

CE 11	Spécifications et protocoles de signalisation *Commission d'études directrice pour la signalisation et les protocoles ainsi que pour les réseaux intelligents*
Etudes se rapportant aux spécifications et protocoles de signalisation pour les fonctions utilisant le protocole Internet (IP), certaines fonctions liées à la mobilité, les fonctions multimédias, et améliorations des Recommandations existantes sur les protocoles d'accès et les protocoles de signalisation interréseau des réseaux ATM, du RNIS à bande étroite et du RTPC. La plupart des Recommandations en vigueur qui ont été élaborées par la CE 11 concernent des réseaux MRT fiables dans lesquels les connexions point à point peuvent être utilisées pour garantir la sécurité des communications. La CE 11 a reconnu que la mise en place de la technologie IP dans le réseau poserait de nouveaux problèmes sur le plan de la sécurité. Compte tenu de la mise en place de la technologie IP et de la nécessité de pouvoir offrir une capacité sécurisée de transmission d'informations de signalisation et de commande dans ce réseau en évolution, la CE 11 a élaboré en 2004 une série de questions liées aux spécifications et aux protocoles de signalisation, destinées à aborder ces nouveaux problèmes sur le plan de la sécurité.	
Questions liées à la sécurité:	
– **Q.1/11** – Architectures fonctionnelles de signalisation et de commande de réseau dans les environnements NGN émergents	
– **Q.7/11** – Spécifications et protocoles de signalisation et de commande pour la prise en charge du rattachement dans les environnements NGN	

CE 12	Qualité de fonctionnement et qualité de service *Commission d'études directrice pour la qualité de service et de fonctionnement*
Etudes se rapportant à la qualité de transmission de bout en bout des terminaux et des réseaux, en rapport avec la qualité perçue et l'acceptabilité par l'utilisateur des applications de texte, de données, de parole et multimédias. Bien que ces travaux couvrent les incidences correspondantes sur la transmission pour tous les réseaux (par exemple, ceux utilisant les systèmes PDH, SDH, ATM et IP ainsi que les réseaux NGN) et tous les terminaux de télécommunication (par exemple, combiné, mains-libres, casque, téléphone mobile, système audiovisuel et réponse vocale interactive), une attention particulière sera accordée à la qualité de service IP, à l'interopérabilité et aux conséquences pour les réseaux NGN, ainsi qu'aux travaux sur la gestion de la qualité de fonctionnement et des ressources.	
Questions liées à la sécurité:	
– **Q.10/12** – Considérations relatives à la planification et à la qualité de la transmission pour les services en bande vocale, de données et multimédias	
– **Q.13/12** – Spécifications de qualité de service et de qualité perçue des services multimédias, et méthodes d'évaluation correspondantes	
– **Q.17/12** – Qualité de fonctionnement des réseaux IP	

CE 13	Réseaux de prochaine génération *Commission d'études directrice pour les réseaux NGN et les questions relatives aux satellites*
Etudes se rapportant à l'architecture, à l'évolution et à la convergence des réseaux de prochaine génération (NGN), y compris les cadres généraux et les architectures fonctionnelles, les spécifications de signalisation applicables aux réseaux NGN, à la coordination de la gestion des projets NGN entre les commissions d'études et à la planification des versions, aux scénarios d'implémentation et aux modèles de déploiement, aux capacités des réseaux et des services, à l'interopérabilité, à l'incidence de l'IPv6, à la mobilité dans les réseaux NGN et à la convergence des réseaux, et aux aspects liés aux réseaux publics de données.	
Reconnaissant que la sécurité est un élément essentiel pour les réseaux NGN, la CE 13 a élaboré une Question portant spécifiquement sur la sécurité, à savoir la Question 15/13 (*Sécurité des réseaux de prochaine génération (NGN)*). Dans le cadre de cette Question, elle s'intéresse aux problèmes de sécurité propres aux réseaux NGN et cherche à élaborer des solutions de sécurité pour ces réseaux. L'un des principaux objectifs de la CE 13 est d'élaborer un ensemble de normes qui garantiront, dans la mesure du possible, la sécurité de l'infrastructure de télécommunication à mesure que les réseaux existants évolueront vers des réseaux NGN. La Commission d'études 13 a aussi décidé d'incorporer dans chaque Recommandation nouvelle ou révisée un paragraphe sur la sécurité afin de mentionner les paragraphes de la Recommandation qui traitent d'aspects de sécurité. Pour ses travaux sur les problèmes de sécurité dans les réseaux NGN, la Commission d'études 13 collabore avec d'autres commissions d'études ainsi qu'avec d'autres organisations de normalisation. L'IETF (domaines de l'Internet, de la sécurité et du transport), les 3GPP et 3GPP2 ainsi que le DSL Forum font partie des organisations de normalisation les plus importantes pour la CE 13 en ce qui concerne ses travaux sur la sécurité.	

Questions liées à la sécurité:

– **Q.2/13** – Prescriptions et scénarios d'implémentation pour les services émergents dans les réseaux NGN
– **Q.3/13** – Principes et architecture fonctionnelle pour les réseaux NGN
– **Q.4/13** – Prescriptions et cadre général de la qualité de service pour les réseaux NGN
– **Q.5/13** – Exploitation, maintenance et gestion des réseaux NGN
– **Q.6/13** – Mobilité dans les réseaux NGN et convergence fixe-mobile
– **Q.7/13** – Interfonctionnement des réseaux et des services dans un environnement de réseaux NGN
– **Q.8/13** – Scénarios de services et modèles de déploiement des réseaux NGN
– **Q.9/13** – Incidence du protocole IPv6 sur un réseau NGN
– **Q.10/13** – Interopérabilité des réseaux satellitaires avec les réseaux de Terre et les réseaux de prochaine génération (NGN)
– **Q.12/13** – Relais de trame (X.272)
– **Q.13/13** – Réseaux publics de données
– **Q.14/13** – Protocoles et mécanismes de services pour les réseaux de données multiservices (MSDN)
– **Q.15/13** – Sécurité des réseaux de prochaine génération (NGN)

Les tâches liées à la sécurité sont les suivantes:

- Diriger le projet relatif à la sécurité des réseaux NGN au sein de la CE 13 et avec les autres commissions d'études. Compte tenu du rôle général de la CE 17 en tant que Commission d'études directrice pour la sécurité des télécommunications, fournir des conseils et une assistance à la CE 17 en ce qui concerne les problèmes de coordination en matière de sécurité des réseaux NGN.
- Déterminer comment appliquer la Rec. UIT-T X.805 (*Architecture de sécurité pour les systèmes assurant des communications de bout en bout*) dans le contexte d'un environnement NGN.
- Veiller à ce que l'architecture élaborée pour les réseaux NGN respecte les principes de sécurité acceptés.
- Veiller à ce que les principes AAA soient correctement intégrés à travers les réseaux NGN.

CE 15	Infrastructures des réseaux optiques et autres réseaux de transport *Commission d'études directrice pour le transport dans le réseau d'accès* *Commission d'études directrice pour les technologies optiques*

La Commission d'études 15 est la commission d'études responsable, à l'UIT-T, de l'élaboration de normes sur les infrastructures, les systèmes et les équipements des réseaux optiques et autres réseaux de transport, les fibres optiques, et les technologies correspondantes du plan de commande, afin de permettre l'évolution vers les réseaux de transport intelligents. A ce titre, elle établit des normes relatives aux sections d'abonné, d'accès, interurbaines et de longue distance des réseaux de communication.

La Question 14/15 porte sur la spécification des prescriptions de gestion et de contrôle et sur la prise en charge de modèles d'information pour les équipements de transport. Elle s'appuie sur le concept de RGT et sur le cadre du RGT établis par l'UIT-T pour la définition de ces prescriptions et de ces modèles. La gestion de la sécurité, qui correspond à l'une des cinq catégories fonctionnelles essentielles de gestion du RGT, est étudiée dans le cadre de la Question 14/15.

a) Prescriptions de gestion des équipements de transport: les Rec. UIT-T G.7710/Y.1701, G.784 et G.874 portent sur les fonctions de gestion d'équipement (EMF, *equipment management function*) qui sont contenues dans un élément de réseau de transport et qui sont respectivement communes à plusieurs techniques, propres aux éléments de réseau SDH et propres aux éléments de réseau OTN. Des applications sont décrites pour la date et l'heure, la gestion des fautes, la gestion de la configuration, la gestion de la comptabilité, la gestion de la qualité et la gestion de la sécurité. Ces applications conduisent à la spécification des fonctions EMF et de leurs prescriptions. Les prescriptions de gestion de la sécurité dans ces Recommandations sont actuellement à l'étude.

b) Architecture et spécification du réseau de communication de données: la Rec. UIT-T G.7712/Y.1703 définit les exigences d'architecture pour un réseau de communication de données (RCD) qui peut accepter les communications de gestion répartie se rapportant au réseau de gestion des télécommunications (RGT), les communications de signalisation répartie se rapportant au réseau optique à commutation automatique (ASON) et les autres communications réparties (par exemple, communications de service ou vocales, téléimportation de logiciel). Diverses applications (par exemple, RGT, ASON, etc.) nécessitent un réseau de communication par paquets afin de transporter les informations entre les différents composants. Par exemple, le RGT a besoin d'un réseau de communication, appelé *réseau de communication de gestion* (RCG) pour transporter les messages de gestion entre les composants du RGT (par exemple, le composant NEF et le composant OSF). L'ASON a besoin d'un réseau de communication, appelé réseau de communication de signalisation (RCS) pour transporter les messages de signalisation entre les composants de l'ASTN (par exemple, les composants CC). La Rec. UIT-T G.7712/Y.1703 fait référence à la série M.3016 concernant les prescriptions de sécurité du réseau RCG. Les prescriptions de sécurité du réseau RCS sont définies dans la Rec. UIT-T G.7712/Y.1703.
c) Gestion répartie des appels et des connexions: la Rec. UIT-T G.7713/Y.1704 spécifie la gestion répartie des appels et des connexions à l'interface utilisateur-réseau (UNI, *user network interface*) et à l'interface de nœud de réseau (NNI, *network node interface*). Elle spécifie plus particulièrement les communications aux interfaces permettant d'effectuer automatiquement les opérations relatives aux appels et aux connexions. Elle spécifie des attributs, notamment des attributs de sécurité permettant de vérifier les opérations relatives aux appels et aux connexions (par exemple, une information permettant d'authentifier la demande d'appel et éventuellement de contrôler l'intégrité de cette demande d'appel).
d) Architecture et prescriptions de routage dans l'ASON: la Rec. UIT-T G.7715/Y.1706 définit les prescriptions et l'architecture pour les fonctions de routage utilisées pour l'établissement des connexions commutées (SC, *switched connection*) et des connexions permanentes logicielles (SPC, *soft permanent connection*) dans le cadre de l'ASON. Parmi les principaux aspects traités dans cette Recommandation, figurent l'architecture de routage ASON et les composants fonctionnels, notamment le choix du chemin, les attributs de routage, les messages abstraits et les diagrammes d'état. Cette Recommandation fait référence aux Recommandations UIT-T de la série M.3016 et à la Rec. UIT-T X.800 concernant les aspects de sécurité. Elle précise notamment que, en fonction des conditions d'utilisation d'un protocole de routage, les objectifs généraux de sécurité définis dans les Recommandations UIT-T de la série M.3016 en matière de confidentialité, d'intégrité des données, de responsabilité et de disponibilité peuvent revêtir différents niveaux d'importance. Pour procéder à une analyse des menaces concernant un protocole de routage envisagé, il faut tenir compte des aspects suivants en s'appuyant sur la Rec. UIT-T X.800: usurpation d'identité, écoute clandestine, accès non autorisé, perte ou altération d'informations (notamment attaque par réexécution), répudiation, falsification et déni de service.
e) Cadre de gestion du réseau ASON: la Rec. UIT-T G.7718/Y.1709 porte sur les aspects de gestion du plan de commande ASON et sur les interactions entre le plan de gestion et le plan de commande ASON. Des prescriptions relatives à la gestion des fautes, à la gestion de la configuration, à la gestion de la comptabilité, à la gestion de la qualité et à la gestion de la sécurité pour les composants du plan de commande seront incluses.
Questions liées à la sécurité:
– **Q.3/15** – Caractéristiques générales des réseaux de transport optiques (G.911)
– **Q.9/15** – Equipements de transport et protection/rétablissement du réseau (G.808.1, G.841, G.842, G.873.1)
– **Q.14/15** – Gestion et commande des systèmes et équipements de transport

CE 16	Terminaux, systèmes et applications multimédias *Commission d'études directrice pour les terminaux, systèmes et applications multimédias ainsi que pour les applications ubiquitaires ("télé-tout", par exemple la télésanté et le commerce électronique)*

La Commission d'études 16 est la Commission d'études directrice pour les terminaux, systèmes et applications multimédias ainsi que pour les applications ubiquitaires ("télé-tout", par exemple la télésanté et le commerce électronique). La Question 25/16 (confiée au GT 2/16), intitulée "Sécurité du multimédia dans les réseaux de prochaine génération", porte sur les problèmes de sécurité suivants.

De graves menaces pèsent sur la sécurité des applications multimédias récentes (par exemple la téléphonie sur les réseaux par paquets, la téléphonie IP, les services interactifs de (visio)conférence et de collaboration; la messagerie multimédia, la transmission audio/vidéo en continu, etc.) dans les environnements hétérogènes. Les mauvaises utilisations, les modifications malveillantes, l'écoute indiscrète et les attaques par déni de service sont des exemples de risques possibles très graves pour la sécurité, notamment dans les réseaux IP.

Il est admis que ces applications ont des besoins de sécurité communs qui peuvent être satisfaits par des mesures de sécurité génériques (sécurité des réseaux, authentification à l'échelle des réseaux, etc.). De plus, les applications multimédias ont généralement des besoins de sécurité qui leur sont propres et pour lesquels le mieux est de prévoir des mesures de sécurité au niveau de la couche application. Dans le cadre de la Question 25/16, on s'intéresse essentiellement aux problèmes de sécurité des applications multimédias au niveau de la couche application dans les réseaux de prochaine génération (NGN-MM-SEC) et on tient compte de moyens complémentaires de sécurité des réseaux si besoin est. L'objet de la Question 25/16 est d'élaborer des Recommandations sur la sécurité qui permettent de répondre aux besoins du marché à cet égard.

Questions liées à la sécurité:

- **Q.1/16** – Systèmes, terminaux et conférence de données multimédias (H.233, H.234)
- **Q.2/16** – Communication audio, vidéo et de données en temps réel sur des réseaux à commutation de paquets (H.323)
- **Q.4/16** – Fonctions évoluées des services de communication multimédia situées au-dessus des plates-formes de système multimédia définies par l'UIT-T (H.350.2)
- **Q.25/16** – Sécurité du multimédia dans les réseaux de prochaine génération (série H.235.x)
- **Q.29/16** – Mobilité pour les systèmes et services multimédias (H.530)

CE 17	Sécurité, langages et logiciels de télécommunication *Commission d'études directrice pour la sécurité des télécommunications ainsi que pour les langages et les techniques de description*

Etudes se rapportant à la sécurité, à l'application des communications entre systèmes ouverts y compris le réseautage et l'annuaire, ainsi qu'aux langages techniques, à leur méthode d'utilisation et à d'autres problèmes connexes liés aux aspects logiciels des systèmes de télécommunication.

La Commission d'études 17 de l'UIT-T est la Commission d'études directrice pour la sécurité des télécommunications. Les travaux de normalisation menés par l'UIT-T dans le domaine de la sécurité sont coordonnés via un nouveau projet de l'UIT-T sur la sécurité géré dans le cadre de la Question 4/17. Dans le cadre de ces travaux, un catalogue des Recommandations de l'UIT relatives à la sécurité et un recueil de définitions relatives à la sécurité extraites des Recommandations de l'UIT-T approuvées ont été élaborés et sont tenus à jour. Des ateliers sur la sécurité et des symposiums sur la cybersécurité ont été tenus en mai 2002 à Séoul (Corée), en octobre 2004 à Florianópolis (Brésil), en mars 2005 à Moscou (Russie) et en octobre 2005 à Genève (Suisse). D'autres ateliers seront organisés en fonction des besoins.

Le GT 1/17 est responsable de la Rec. UIT-T X.509 (*Cadre général des certificats de clé publique et d'attribut*), qui jette les bases des infrastructures de clé publique (PKI, *public key infrastructure*) et des infrastructures de gestion de privilège (PMI, *privilege management infrastructure*). Cette Recommandation continue à être améliorée pour répondre à l'évolution des besoins. Le GT 2/17 est responsable des Recommandations relatives aux architectures, aux cadres généraux et aux protocoles de sécurité essentiels établis, notamment des Recommandations de la série X.800. Au cours de la dernière période d'études, un ensemble de nouvelles Recommandations relatives à la sécurité ont été élaborées, dont la Rec. UIT-T X.805 qui définit une architecture de sécurité pour assurer la sécurité du réseau de bout en bout. Cette architecture peut être appliquée à divers types de réseaux, indépendamment de la technologie sous-jacente du réseau. Elle peut servir d'outil pour faire en sorte que la sécurité soit correctement prise en compte lorsqu'il s'agit d'élaborer des Recommandations ou de réaliser des évaluations de sécurité des réseaux. Une autre Recommandation fondamentale, X.1051, spécifie un système de gestion de la sécurité de l'information (ISMS, *information security management system*) dans le contexte des télécommunications. Elle expose les conditions de mise en place, d'implémentation, d'exploitation, de supervision, de réexamen, de maintenance et d'amélioration d'un système ISMS documenté dans le contexte des risques globaux afférents aux activités des organisations de télécommunications. La Rec. UIT-T X.1081 est une Recommandation cadre qui jette les bases des futures spécifications sur la télébiométrie. Les Rec. UIT-T X.1121 et X.1122 portent sur les communications mobiles de données de bout en bout. La Rec. UIT-T X.1121 analyse les menaces de sécurité dans un environnement mobile et les moyens de protection du point de vue de l'utilisateur mobile et du fournisseur de services d'application. La Rec. UIT-T X.1122 donne des indications pour la construction de systèmes mobiles sécurisés fondés sur la technologie de l'infrastructure de clé publique (PKI, *public key infrastructure*). Les informations à jour figurent sur la page de la CE 17 du site web de l'UIT (voir http://www.itu.int/ITU-T/studygroups/com17/tel-security.html).

Questions liées à la sécurité:

GT 1/17 Technologie des systèmes ouverts

– **Q.1/17 –** Communications en multidiffusion de bout en bout avec fonctionnalité de gestion de la qualité de service

Cette Question porte sur les exigences, l'architecture, la gestion de groupe et de session ainsi que le protocole de communications en multidiffusion pour les communications en multidiffusion de bout en bout. Afin d'assurer la sécurité des communications de groupe entre les membres, on s'intéresse aux extensions de sécurité relatives aux protocoles de communication en multidiffusion de bout en bout. Les travaux en cours portent sur l'application de mécanismes de sécurité aux protocoles de communication en multidiffusion et sur l'élaboration de procédures pour assurer la sécurité des communications.

– **Q.2/17** – Services d'annuaire, systèmes d'annuaire et certificats d'attributs et de clés publiques

Cette Question a notamment pour objet le développement et la tenue à jour de la Rec. UIT-T X.509, qui porte sur les certificats de clé publique, les certificats d'attribut, la révocation de certificats et la spécification des infrastructures sous-jacentes (infrastructure de clé publique et infrastructure de gestion de privilège). Les certificats de clé publique et l'infrastructure sous-jacente sont fondamentaux pour l'authentification et sont notamment appliqués pour les signatures numériques.

– **Q.16/17** – Noms de domaine internationalisés

Des problèmes de sécurité se posent dans le cadre des travaux sur les noms de domaine internationalisés. La Question 16/17 vise en particulier à identifier les documents techniques existants qui énoncent les principes régissant les noms IDN, y compris les documents relatifs aux risques qu'entraîne l'implémentation de noms IDN pour la sécurité des réseaux de télécommunication. Cette tâche est effectuée en consultation avec les organismes compétents (ISO/CEI, Consortium UNICODE, IETF, ICANN et CENTR).

GT 2/17 Sécurité des télécommunications

– **Q.4/17** – Projet relatif à la sécurité des systèmes de communication

Cette Question vise à fixer de grands principes mais aussi à assurer la coordination et l'organisation de toute la gamme des activités à déployer dans le domaine de la sécurité des communications à l'UIT-T. La méthode descendante sera utilisée en collaboration avec d'autres commissions d'études et d'autres organisations de normalisation. Ce projet vise à mettre en place une méthode plus ciblée au niveau des projets et des stratégies.

– **Q.5/17** – Architecture et cadre général de la sécurité

Pour obtenir des solutions sécuritaires complètes et rentables qui puissent s'appliquer à différents types de réseaux, de services et d'applications, dans un environnement où existent plusieurs fabricants, il faut que la sécurité du réseau s'articule sur des architectures et des technologies de sécurité normalisées. Compte tenu des dangers qui menacent la sécurité du secteur de la communication et des progrès réalisés dans le domaine des contre-mesures de protection, ce projet a pour objet d'explorer les nouveaux besoins en matière de sécurité ainsi que leurs solutions et de déterminer comment élaborer des architectures et des cadres de sécurité qui tiennent compte de l'évolution de l'environnement.

– **Q.6/17** – Cybersécurité

Cette Question porte sur la cybersécurité dans le contexte de la normalisation internationale. Elle vise en particulier à étudier les points suivants:

- processus de distribution, de partage et de divulgation des informations sur la vulnérabilité;
- procédure normalisée pour les opérations de prise en charge des incidents dans le cyberespace;
- stratégie de protection de l'infrastructure critique du réseau.

– **Q.7/17** – Gestion de la sécurité

Cette Question a pour objet d'élaborer un ensemble de Recommandations sur la gestion de la sécurité pour l'UIT-T, compte tenu de la nécessité de collaborer avec l'ISO/CEI JTC 1. En particulier, elle porte sur l'identification et la gestion du risque dans les systèmes de télécommunication et vise à aligner sur les normes existantes de système de gestion de la sécurité des informations (ISMS, *information security management system*) le système ISMS destiné aux exploitants de télécommunication.

– **Q.8/17** – Télébiométrie

L'étude de cette Question, qui s'appuie sur les travaux existants concernant l'identification et l'authentification des personnes au moyen de la télébiométrie, est réalisée en étroite coopération avec d'autres organisations de normalisation qui effectuent des travaux de normalisation connexes. Cette Question vise notamment à déterminer comment améliorer l'identification et l'authentification des utilisateurs par l'utilisation de méthodes sécurisées de télébiométrie et comment identifier les problèmes liés aux technologies d'authentifications biométriques pour les télécommunications.

– **Q.9/17** – Services de communication sécurisés

Compte tenu de certaines caractéristiques spécifiques des communications mobiles (par exemple, transmission hertzienne, puissance de calcul et taille de mémoire limitées des petits dispositifs mobiles), assurer la sécurité est une tâche particulièrement difficile qui mérite une attention et une étude particulières. Cette Question vise à déterminer comment les services de communication sécurisés peuvent être identifiés et définis dans les services de communications mobiles ou les services web, comment les menaces qui pèsent sur les services de communication peuvent être identifiées et prises en charge, les technologies qui permettent de prendre en charge les services de communication sécurisés et comment une interconnectivité sécurisée entre les systèmes de communication peut être maintenue.

– **Q.17/17** – Lutter contre le spam par des moyens techniques

Cette Question porte sur les besoins techniques, les cadres, les lignes directrices et les nouvelles technologies pour lutter contre le spam. Elle vise notamment à élaborer un ensemble de Recommandations sur la lutte contre le spam dans les systèmes de messagerie électronique et dans les applications multimédias, compte tenu du besoin de collaboration avec les autres commissions d'études de l'UIT-T et avec d'autres organisations de normalisation.

GT 3/17 Langages et logiciels de télécommunication

– **Q.10/17** – Notation de syntaxe abstraite numéro un (ASN.1) et autres langages de données

Cette Question a pour objet de mettre à jour et d'améliorer la notation ASN.1 et ses règles de codage, dont les règles de codage distinctives (DER, *distinguished encoding rules*) qui sont utilisées pour la création de certificats numériques ou de signatures numériques X.509. La notation ASN.1 joue un rôle important dans la représentation des informations sous une forme qui puisse être chiffrée/déchiffrée et signée/vérifiée de façon fiable. La notation ASN.1 doit continuer d'être améliorée pour répondre à l'évolution des besoins dans les environnements de communication actuels.

CE 19	Réseaux de télécommunication mobiles *Commission d'études directrice pour les réseaux de télécommunication mobiles et la mobilité*
Etudes se rapportant aux aspects "réseau" des réseaux de télécommunication mobiles, y compris les télécommunications mobiles internationales 2000 (IMT-2000) et les systèmes postérieurs aux IMT-2000, l'Internet sans fil, la convergence des réseaux mobiles et fixes, la gestion de la mobilité, les fonctions multimédias mobiles, l'interréseautage, l'interopérabilité et l'amélioration des Recommandations UIT-T existantes sur les IMT-2000.	
Questions liées à la sécurité:	
– **Q.1/19** – Besoins en matière de capacités de service et de capacités de réseau et architecture de réseau	
– **Q.3/19** – Identification des systèmes IMT-2000 existants ou en évolution (Q.1741.1, Q.1741.2, Q.1741.3, Q.1742.1, Q.1742.2, Q.1742.3)	
– **Q.5/19** – Convergence des réseaux IMT-2000 en évolution et des réseaux fixes en évolution	

Modules de sécurité de l'UIT-T

Cadre de l'architecture de sécurité

X.800 – Architecture de sécurité
X.802 – Modèle de sécurité des couches inférieures
X.803 – Modèle de sécurité des couches supérieures
X.810 – Cadres de sécurité pour les systèmes ouverts: aperçu général
X.811 – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification
X.812 – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès
X.813 – Cadres de sécurité pour les systèmes ouverts: cadre de non-répudiation
X.814 – Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité
X.815 – Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité
X.816 – Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité

Sécurité des télécommunications

X.805 – Architecture de sécurité pour les systèmes assurant des communications de bout en bout
X.1051 – Système de gestion de la sécurité de l'information – Prescriptions pour les télécommunications (ISMS-T)
X.1081 – Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie
X.1121 – Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout
X.1122 – Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI)

Protocoles

X.273 – Protocole de sécurité de la couche Réseau
X.274 – Protocole de sécurité de la couche Transport

Sécurité en mode relais de trame

X.272 – Compression et secret des données dans les réseaux à relais de trames

Techniques de sécurité

X.841 – Objets informationnels de sécurité pour le contrôle d'accès
X.842 – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance
X.843 – Spécification des services de tiers de confiance pour la prise en charge des applications de signatures numériques

Services d'annuaire et authentication

X.500 – Aperçu général des concepts, modèles et services
X.501 – Les Modèles
X.509 – Cadre général des certificats de clé publique et d'attribut
X.519 – Spécification des protocoles

Sécurité de gestion de réseau

M.3010 – Principes du réseau de gestion des télécommunications
M.3016.x – Sécurité du RGT (sous-série de Recommandations)
M.3210.1 – Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000
M.3320 – Cadre général des prescriptions de gestion pour l'interface X du réseau de gestion des télécommunications
M.3400 – Fonctions de gestion RGT

Gestion des systèmes

X.733 – Fonction de signalisation des alarmes
X.735 – Fonction de commande des registres de consignation
X.736 – Fonction de signalisation des alarmes de sécurité
X.740 – Fonction de piste de vérification de sécurité
X.741 – Objets et attributs de contrôle d'accès

Systèmes de télévision et systèmes de transmission par câble

J.91 – Méthodes techniques pour garantir la confidentialité sur les transmissions internationales de télévision à grande distance
J.93 – Prescriptions d'accès conditionnel dans le réseau de distribution secondaire de la télévision numérique par câble
J.170 – Spécification de la sécurité sur IPCablecom

Communications multimédias

H.233 – Système de confidentialité pour les services audiovisuels
H.234 – Gestion des clés de chiffrement et système d'authentification pour les services audiovisuels
H.235.x – Cadre de sécurité H.323 (sous-série de Recommandations)
H.323 Annexe J – Systèmes de communication multimédia en mode paquet – Sécurisation des dispositifs de l'Annexe F/H.323 (Sécurisation des dispositifs d'extrémité simples)
H.350.2 – Architecture des services d'annuaire pour les systèmes H.235
H.530 – Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510

Télécopie

T.30 Annexe G – Procédures pour la transmission sécurisée de documents de télécopie du Groupe 3 utilisant les systèmes HKM et HFX
T.30 Annexe H – Sécurisation de la télécopie G3 sur la base de l'algorithme RSA
T.36 – Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3
T.503 – Profil d'application de document pour le transfert de documents de télécopie du Groupe 4
T.563 – Caractéristiques des télécopieurs du Groupe 4

Systèmes de messagerie

X.400/F.400 – Aperçu général du système et du service de messagerie
X.402 – Architecture globale
X.411 – Système de transfert de messages: définition et procédures du service abstrait
X.413 – Mémoire de messages – Définition du service abstrait
X.419 – Spécification des protocoles
X.420 – Système de messagerie de personne à personne
X.435 – Système de messagerie par échange informatisé de données
X.440 – Système de messagerie vocale

Les Recommandations de l'UIT-T sont accessibles sur le site web de l'UIT à l'adresse http://www.itu.int/publications/bookshop/how-to-buy.html (on trouvera également sur cette page des informations concernant l'accès gratuit à un nombre limité de Recommandations de l'UIT).

Les sujets importants que l'UIT-T traite actuellement du point de vue de la sécurité sont les suivants:

Télébiometrie, gestion de la sécurité, sécurité de la mobilité, cybersécurité, sécurité des réseaux domestiques, sécurité des réseaux de prochaine génération, lutte contre le pollupostage et télécommunications d'urgence

Pour plus d'informations sur l'UIT-T et sur ses Commissions d'études, on se reportera à l'adresse: http://www.itu.int/ITU-T

Imprimé en Suisse
Genève, 2006